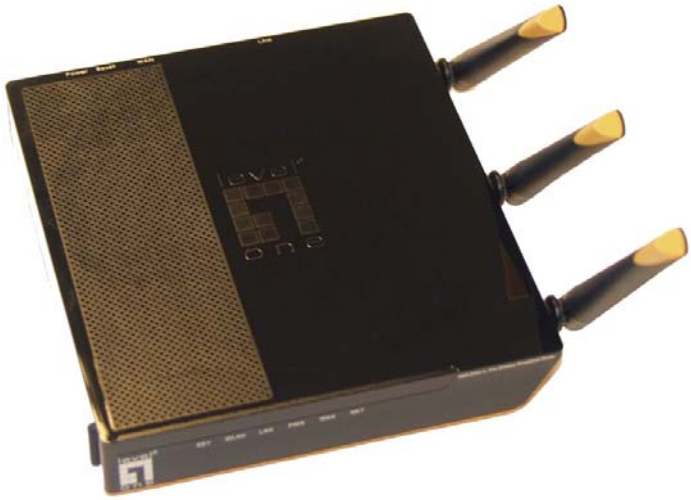
WBR-6000

N-One WLAN-Breitbandrouter



Benutzerhandbuch

Digital Data Communications GmbH
Zeche-Norm-Str. 25
44319 Dortmund

Technische Support Hotline: 01805-991002
E-Mail: support@level-one.de
Internet:www.level-one.de

V1.0.0-0705

Inhaltsverzeichnis

1. EINLEITUNG 1
1.1. Lieferumfang 1
1.2. Funktionen des WLAN-Breitbandrouters 2
1.2.1. Funktionen des Internetzugangs 2
1.2.2. Erweiterte Internetfunktionen 2
1.2.3. WLAN-Funktionen 4
1.2.4. LAN-Funktionen 4
1.2.5. Konfiguration und Verwaltung 5
1.2.6. Sicherheitsfunktionen 5
2. INFORMATIONEN ZU DIESER ANLEITUNG 6
2.1. Zweck und Ziel 6
2.2. Marken und Markenzeichen 6
2.3. Nachweis verwendeter Informationen 6
2.4. Haftung 7
2.5. Fachbegriffe 7
2.6. Abbildungen 8
2.7. Druck dieser Anleitung 8
2.8. Verwendete graphische Symbole 9
3. SICHERHEITSHINWEISE 10
3.1. Bestimmungsgemäße Verwendung 10
3.2. Bestimmungswidrige Verwendung 11
3.3. Elektrische Spannung 11
3.4. Steckernetzteil 12
3.5. Blitzschlag und Überspannung 12
3.6. Aufstellort und Umgebungsbedingungen 13
3.7. Temperatur 13
3.8. Feuchtigkeit 13
3.9. Vorsichtsmaßnahmen zum Schutz von Kindern 13
3.10. Zielgruppe und Anforderungen an den Benutzer 14
3.11. Potentielle finanzielle Schadensrisiken 14
3.11.1. Ungewollte Online-Verbindungsgebühren 14
3.11.2. Ausfall des IT-Systems 15
3.11.3. Ausfall der Internetverbindung 15
3.11.4. Vorsicht bei Firmware-Upgrades 15
3.11.5. Notwendige Maßnahmen zum Schutz Ihres Netzwerkes 16
4. TECHNISCHE DETAILS 17
4.1. LEDs an der Vorderseite 17
4.2. Rückseite des Geräts 18
5. INSTALLATION 19
5.1. Voraussetzungen 19
5.2. Vorgehensweise 19

6. SETUP 21
6.1. Übersicht 21
6.2. Konfigurationsprogramm 23
6.2.1. Vorbereitung 23
6.2.2. Verwendung des Web-Browsers 23
6.2.3. Verbindungsaufbau nicht möglich 24
6.3. Einrichtungsassistent 25
6.3.1. Gebräuchliche Verbindungsarten 26
6.4. Bildschirmanzeige Home 28
6.4.1. Hauptmenü 29
6.4.2. Navigation und Dateneingabe 29
6.5. Bildschirmanzeige LAN 30
6.5.1. Daten - Bildschirmanzeige LAN 31
6.5.2. DHCP 32
6.5.3. Bildschirmanzeige Wireless 34
6.6. WLAN-Sicherheit 38
6.6.1. WEP WLAN-Sicherheit 38
6.6.2. WPA-PSK WLAN-Sicherheit 40
6.6.3. WPA2-PSK WLAN-Sicherheit 41
6.6.4. WPA-PSK+WPA2-PSK WLAN-Sicherheit 42
6.7. Bildschirmanzeige Passwort 43
7. PC-KONFIGURATION 44
7.1. Übersicht 44
7.2. Windows-Clients 44
7.2.1. TCP/IP-Einstellungen - Übersicht 44
7.2.2. Überprüfen der TCP/IP-Einstellungen - Windows 9x/ME 46
7.2.3. Überprüfen der TCP/IP-Einstellungen - Windows 2000 49
7.2.4. Überprüfen der TCP/IP-Einstellungen - Windows XP 51
7.2.5. Internetzugang 53
7.3. Macintosh-Clients 55
7.4. Linux-Clients 55
7.5. Andere Unix-Systeme 56
7.6. Konfiguration der WLAN-Stationen 56
8. BETRIEB UND STATUS 57
8.1. Betrieb 57
8.2. Statusanzeige 57
Daten - Statusanzeige 57
8.3. Verbindungsstatus - PPPoE 60
8.4. Verbindungsstatus - PPTP 62
8.5. Verbindungsstatus - L2TP 64
8.6. Verbindungsstatus – Telstra Big Pond 66
8.7. Verbindungsdetails - SingTel RAS 68
8.8. Verbindungsdetails - Dynamische IP-Adresse 70
8.9. Verbindungsdetails - Statische IP-Adresse 72

9. ERWEITERTE FUNKTIONEN ... 73
9.1. Übersicht ... 73
9.2. Internet ... 73
9.2.1. DMZ ... 74
9.2.2. URL-Filter ... 74
9.3. Zugriffskontrolle ... 76
9.3.1. Übersicht ... 76
9.3.2. Bildschirmanzeige Zugriffskontrolle ... 76
9.3.3. Bildschirmanzeige Privilegierte PCs ... 78
9.4. Dynamischer DNS (Domain Name Server) ... 79
9.4.1. Bildschirmanzeige DDNS ... 79
9.5. Firewall-Regeln ... 81
9.5.1. Bildschirmanzeige Firewall-Regeln ... 81
9.5.2. Eingangsregeln (eingehende Dienste) ... 84
9.5.3. Ausgangsregeln (ausgehende Dienste) ... 87
9.6. Firewall-Dienste ... 90
9.7. Virtuelle Server ... 91
9.7.1. IP-Adresse ist für Internetnutzer einsehbar ... 91
9.7.2. Bildschirmanzeige Virtuelle Server ... 92
9.7.3. Definition Ihrer eigenen virtuellen Server ... 94
9.7.4. Verbindungsaufbau zu den virtuellen Servern ... 95
9.8. Optionen ... 96
9.9. Port Trigger ... 98
9.10. Zeitpläne ... 99
10. ERWEITERTE VERWALTUNG ... 101
10.1. Übersicht ... 101
10.2. PC-Datenbank ... 102
10.2.1. Bildschirmanzeige PC-Datenbank ... 102
10.3. Diagnose ... 103
10.4. Konfigurationsdatei ... 104
10.5. Logs ... 105
10.6. Externe Verwaltung ... 106
10.7. Firmware-Upgrade ... 108
11. FEHLERSUCHE UND -BEHEBUNG ... 109
11.1. Übersicht ... 109
11.2. Allgemeine Probleme ... 109
11.3. Internetzugang ... 110
11.4. WLAN-Zugang ... 111
12. WIRELESS LANS ... 113
12.1. Modi ... 113
12.2. BSS/ESS ... 113
12.3. Kanäle ... 114
12.4. WEP ... 114
12.5. WPA-PSK ... 115
12.6. Konfiguration des Wireless LAN ... 116

13. SPEZIFIKATIONEN 117
13.1. Multifunktionaler WLAN-Breitbandrouter 117
13.2. WLAN-Schnittstelle 117
14. ENTSORGUNG 118
15. GNU GENERAL PUBLIC LICENSE 119

Copyright

Der Inhalt dieser Publikation darf ohne schriftliche Zustimmung weder in Teilen noch vollständig in irgendeiner Form vervielfältigt, veröffentlicht oder in andere Sprachen übersetzt werden.

Marken und Warenzeichen

LevelOne und das LevelOne-Logo sind eingetragene Warenzeichen der Digital Data Communications GmbH. Andere Markennamen und Warenzeichen, die zum Zwecke der eindeutigen Identifikation in diesem Dokument genannt werden, sind in der Regel Warenzeichen der entsprechenden Firmen. Änderung der Angaben ohne vorherige Ankündigung sind vorbehalten.

FCC-Interferenzkonformität

Eine Prüfung der Geräte hat ergeben, dass die Grenzwerte für Digitalgeräte der Klasse B gemäß Teil 15 der FCC-Regeln eingehalten werden. Diese Grenzwerte wurden festgelegt, um ausreichenden Schutz vor Funkstörung in kommerzieller Umgebung zu gewährleisten. Diese Geräte können Hochfrequenzenergie erzeugen, nutzen und abstrahlen. Die Missachtung der Anweisungen für Installation und Betrieb in diesem Benutzerhandbuch kann Störungen der Fernmeldekommunikation zur Folge haben. Bei Betrieb dieser Geräte in häuslicher Umgebung kommt es mit großer Wahrscheinlichkeit zu Interferenzen. Der Benutzer muss die Kosten für erforderliche Maßnahmen zum Ausgleich dieser Interferenzen selbst tragen.

CE-Konformitätserklärung

Diese Geräte erfüllen alle Anforderungen im Hinblick auf elektromagnetische Verträglichkeit gemäß der Richtlinien 73/23/EWG, 89/336/EWG und 99/5/EG.
Dieses Gerät ist vorgesehen für die Verwendung in Wohnbereichen, Gewerbe- und Geschäftsbereichen sowie Kleinbetrieben. Es ist nicht vorgesehen für die Verwendung in Industriebereichen.
Änderung der Angaben ohne vorherige Ankündigung sind vorbehalten.
Hiermit erklärt Digital Data Communications, dass sich das Gerät WBR-6000 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Die EG-Konformitätserklärung ist einsehbar unter: http://www.level-one.de/support.php

Abb. 1 Typenschild WBR-6000

1. Einleitung

Dieses Kapitel gibt einen Überblick über Merkmale und Funktionen des WLAN-Breitbandrouters.

Wir gratulieren Ihnen zum Kauf des WLAN-Breitbandrouters. Der WLAN-Breitbandrouter ist ein multifunktionales Gerät mit folgenden Funktionen:

- ***Gemeinsam genutzter Breitband-Internetzugang*** für alle LAN-Benutzer.
- ***4-Port Switching Hub*** für 10BaseT- oder 100BaseT-Verbindungen.

1.1. Lieferumfang

Die folgenden Gegenstände sollten sich in Ihrem Paket befinden. Sollte einer der Artikel fehlen oder beschädigt sein, kontaktieren Sie bitte umgehend Ihren Händler.

- WBR-6000
- Cat.5-Kabel
- Netzteil
- Schnellinstallationsanleitung
- Handbuch auf CD-ROM

Abb. 2 Lieferumfang

Sollte einer der oben erwähnten Artikel fehlen oder beschädigt sein, kontaktieren Sie bitte umgehend Ihren Händler.

1.2. Funktionen des WLAN-Breitbandrouters

Ihr WLAN-Breitbandrouter verfügt über viele fortschrittliche Leistungsmerkmale; trotz seiner vielen Funktionen ist das Gerät einfach zu bedienen.

1.2.1. Funktionen des Internetzugangs

- ***Gemeinsam genutzter Internetzugang***
  Alle Nutzer im LAN oder WLAN können unter Nutzung einer einzigen externen IP-Adresse über den WLAN-Breitbandrouter auf das Internet zugreifen. Die lokalen (ungültigen) IP-Adressen sind vor externen Quellen verdeckt. Dieser Prozess nennt sich NAT (Network Address Translation).
- ***DSL- & Kabelmodem-Unterstützung***
  Der WLAN-Breitbandrouter verfügt über einen 10/100BaseT-Ethernert-Port für den Anschluss von DSL- oder Kabelmodems. Alle gängigen DSL- und Kabelmodems werden unterstützt. SingTel RAS- und Big Pond (Australien)-Login-Unterstützung ist ebenfalls eingeschlossen.
- ***PPPoE-, PPTP-, SingTel RAS- und Telstra Big Pond-Unterstützung***
  Die Internetverbindung (WAN-Port) unterstützt PPPoE (PPP über Ethernet), PPTP (Peer-to-Peer Tunneling Protocol), L2TP, SingTel RAS und Telstra Big Pond (Australien) sowie „Direct Connection“-Dienste. Außerdem werden unnummerierte IPs mit PPPoE unterstützt.
- ***Feste oder dynamische IP-Adresse***
  Bei der Internetverbindung (WAN-Port) unterstützt der WLAN-Breitbandrouter sowohl dynamische (die IP-Adresse wird beim Verbindgungsaufbau zugeordnet) als auch feste IP-Adressen.

1.2.2. Erweiterte Internetfunktionen

- ***URL-Filter***
  Verwenden Sie den URL-Filter, um LAN-Nutzer daran zu hindern, unerwünschte Websites aufzusuchen.
- ***DMZ***
  Mit jeder WAN-IP-Adresse (Internet), die Ihnen zugeteilt wird, kann ein PC in Ihrem LAN so konfiguriert werden, dass er uneingeschränkte wechselseitige Kommunikation mit den Servern oder Einzelnutzern im Internet zulässt. Dies macht es möglich, Programme ablaufen zu lassen, die nicht mit Firewalls kompatibel sind.
- ***Zugriffskontrolle***
  Mit diesem Feature können Sie bestimmen, auf welche Internetdienste die LAN-Nutzer zugreifen können.
- ***Unterstützung von Dynamischem DNS***
  Wenn DDNS zusammen mit dem Virtual Server-Feature verwendet wird, können Anwender mit einem Domainnamen auf Server in Ihrem LAN zugreifen, selbst wenn Sie über eine dynamische IP-Adresse verfügen, die sich bei jeder erneuten Verbindung ändert.

- ***Firewall***
  Neben der integrierten Firewall, die Ihr LAN schützt, können Sie selber Firewallregeln festlegen, um zu bestimmen, welche Art von ein- oder ausgehendem Datenverkehr erlaubt ist.
- ***Firewall-Dienste***
  Anwendungen, die nichtstandardisierte Verbindungen oder Portnummern nutzen, werden im Normalfall von der Firewall blockiert. Solche Anwendungen können zugelassen werden, um sie normal nutzen zu können.
- ***Port Trigger***
  Mit dieser Funktion können Sie Internetanwendungen benutzen, die normalerweise nicht funktionieren, wenn Sie hinter einer Firewall verwendet werden.
- ***Zeitablaufsteuerung***
  Die Regeln für den URL-Filter und die Firewall können so eingerichtet werden, dass Sie nur zu bestimmte Zeiten aktiv sind. Dadurch wird die Flexibilität bei der Steuerung von Datenverkehr über das Internet vergrößert.
- ***Virtuelle Server***
  Mit diesem Feature können Internetnutzer auf die Internetserver auf Ihrem LAN zugreifen. Das dazu benötigte Setup ist schnell und einfach.
- ***VPN-Pass-through-Unterstützung***
  PCs mit VPN-Software (Virtual Private Networking), die PPTP, L2TP und IPSec nutzen, werden transparent unterstützt – es ist keine Konfiguration notwendig.
- ***Log-Dateien***
  Hier können Sie festlegen, welche Art von Daten in Logs festgehalten wird. Optional können Sie Logdaten an einen Syslog-Server schicken oder die Logdaten per E-Mail erhalten.

1.2.3. WLAN-Funktionen

- ***Standardkonformität***
  Der WLAN-Breitbandrouter ist konform mit den Spezifikationen der IEEE802.11g (DSSS) für Wireless LANs.
- ***Unterstützung von Pre-N WLAN-Stationen***
  Der Entwurf 802.11n garantiert Abwärtskompatibilität mit dem Standard 802.11b, sodass WLAN-Stationen nach 802.11b und 802.11g gleichzeitig verwendet werden können.
- ***Geschwindigkeit bis zu 300Mbps***
  Alle Geschwindigkeiten bis zum Entwurf 802.11n mit einem Maximum von 300 Mbps werden unterstützt.
- ***WEP-Unterstützung***
  WEP (Wired Equivalent Privacy) wird unterstützt. Es werden Schlüsselgrößen von 64 Bit und 128 Bit unterstützt. WEP verschlüsselt Daten vor der Übertragung, sodass sie vor „Schnüfflern“ geschützt sind.
- ***WPA-PSK-Unterstützung***
  Genau wie WEP verschlüsselt auch WPA-PSK Daten vor der Übertragung, sodass sie vor „Schnüfflern“ geschützt sind. WPA-PSK ist ein aktuellerer Standard als WEP. Die Vorteile sind sowohl die einfachere Konfiguration als auch die größere Sicherheitsstufe.
- ***WPA2-PSK-Unterstützung***
  Auch WPA2-PSK wird unterstützt. WPA2-PSK verwendet die äußerst sichere AES-Verschlüsselung.
- ***Wireless MAC Access Control***
  Die Funktion Wireless Access Control überprüft die MAC-Adresse (Hardware-Adresse) von WLAN-Stationen, um damit sicherzustellen, dass der Zugriff auf Ihr LAN nur von WLAN-Station aus erfolgen kann, denen Sie vertrauen können.
- ***Einfache Konfiguration***
  Sollten die Werksvoreinstellungen für Ihre Anwendungen ungeeignet sein, können diese schnell und einfach geändert werden.

1.2.4. LAN-Funktionen

- ***4-Port Switching Hub***
  Der WLAN-Breitbandrouter ist mit einem 4-Port 10/100BaseT Switching Hub ausgestattet, über den Sie ein LAN aufbauen oder erweitern können.
- ***DHCP-Serverunterstützung***
  Das **D**ynamic **H**ost **C**onfiguration **P**rotocol vergibt eine dynamische IP-Adresse an PCs und auf Wunsch auch an andere Geräte. Der WLAN-Breitbandrouter kann als **DHCP-Server** für Geräte auf Ihrem lokalen LAN und WLAN fungieren.

1.2.5. Konfiguration und Verwaltung

- ***Upload / Download der Konfigurationsdatei***
  Speichern Sie die Konfigurationsdaten des WLAN-Breitbandrouters auf Ihrem PC (Download) bzw. schicken Sie eine dort gespeicherte Konfigurationsdatei zum WLAN-Breitbandrouter (Upload).
- ***Externe Verwaltung***
  Der WLAN-Breitbandrouter kann von jedem PC in Ihrem LAN oder Wireless LAN aus verwaltet werden. Bei bestehender Internetverbindung kann er (optional) ebenso über das Internet konfiguriert werden.
- ***Diagnose***
  Nutzen Sie den WLAN-Breitbandrouter außerdem für die Funktionen *Ping* oder *DNS Lookup*.
- ***UPnP-Unterstützung***
  UPnP (Universal Plug and Play) ermöglicht das automatische Lokalisieren und Konfigurieren des WLAN-Breitbandrouters. UPnP wird von Windows ME, XP, oder späteren Versionen unterstützt.

1.2.6. Sicherheitsfunktionen

- ***Passwortgeschützte Konfiguration***
  Durch den Passwortschutz werden nicht autorisierte Anwender daran gehindert, Konfigurationsdaten und Einstellungen zu ändern.
- ***WLAN-Sicherheit***
  Auch WPA/WPA2-PSK, WEP und die Funktion Wireless Access Control werden unterstützt. Dadurch werden unbekannte WLAN-Stationen daran gehindert, auf Ihr LAN zuzugreifen.
- ***NAT-Schutz***
  Als Nebeneffekt der NAT-Technologie (Network Address Translation) können LAN-Nutzer eine gemeinsame IP-Adresse verwenden, wobei der Standort und jeder einzelne PC verborgen ist. Ein externer Betrachter sieht kein Netzwerk, sondern lediglich ein einziges Gerät - den WLAN-Breitbandrouter.
- ***Firewall***
  Alle eingehenden Datenpakete werden geprüft und alle eingehenden Serveranfragen gefiltert, um Ihr Netzwerk vor böswilligen Angriffen von außen zu schützen.
- ***Schutz gegen DoS-Angriffe***
  DoS-Angriffe (Denial of Service) können Ihre Internetverbindung mit ungültigen Paketen und Verbindungsanfragen überschwemmen und damit die verfügbare Bandbreite und Kapazität so in Anspruch nehmen, dass der Internetzugang nicht mehr zur Verfügung steht. Der WLAN-Breitbandrouter schützt Sie gegen DoS-Angriffe.

2. Informationen zu dieser Anleitung

2.1. Zweck und Ziel

Diese Anleitung informiert Sie über

- ✓ den bestimmungsgemäßen Verwendungsbereich
- ✓ die ordnungsgemäße Inbetriebnahme des Routers

Sie erhalten außerdem wichtige Hinweise für den

- ✓ sicheren Gebrauch des Routers und werden vor möglichen Risiken gewarnt, die durch Nichtbeachtung dieser Hinweise entstehen können.

2.2. Marken und Markenzeichen

LevelOne und das LevelOne-Logo sind eingetragene Warenzeichen der Digital Data Communications GmbH. Andere Markennamen oder Warenzeichen, die zum Zwecke der eindeutigen Identifikation in diesem Dokument erwähnt werden, sind in der Regel Warenzeichen der entsprechenden Firmen.

2.3. Nachweis verwendeter Informationen

In der Erarbeitung der Sicherheitshinweise wurden unter anderem die Ausführungen des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutzhandbuchs (Stand Oktober 2003) berücksichtigt. Aufgrund des beschränkten Raumes, der im Rahmen einer Anleitung zur Verfügung steht, kann hier nur eine Auswahl der in der Praxis unter Umständen relevanten Aspekte dargestellt werden. Zusätzlich wird deswegen empfohlen, weitergehende Informationen aus den für den jeweiligen Anwendungsfall einschlägigen Abschnitten des IT-Grundschutzhandbuches, insbesondere des Gefährdungskataloges, zu beziehen:

http://www.bsi.bund.de/gshb/deutsch/menue.htm

Für die kriminologischen Erläuterungen zu Fachausdrücken wurden Fachliteratur sowie einschlägige Online-Quellen hinzugezogen, u. a. Themen aus dem Diskussionsforum de.com.security.

2.4. Haftung

- ✓ Der Inhalt dieser Installationsanleitung wurde auf der Grundlage von Fachinformationen, detaillierter Anwendungsanalyse des Installations-Vorganges und Erfahrungen von Anwendern mit größter Sorgfalt erarbeitet.
- ✓ Digital Data Communications GmbH behält sich das Recht vor, Änderungen dieses Routers, die entweder Hardware- oder Softwarekomponenten (Firmware) betreffen können, im Interesse der Weiterentwicklung und der Verbesserung von Funktionalität und Zuverlässigkeit des Produktes ohne vorherige Ankündigung durchzuführen.
  Die Beschreibungen und Abbildungen basieren auf dem Informationsstand zum Zeitpunkt der Erstellung dieses Dokumentes (Juli 2007).
- ✓ Ebenso behält sich der Herausgeber dieser Anleitung, die Digital Data Communications GmbH, das Recht vor, Korrekturen und Änderungen am Inhalt dieses Dokumentes ohne vorherige Ankündigung durchzuführen. Die jeweils aktuelle Dokumentation finden Sie unter:
  http://www.level-one.de/support.php

Aus den nachfolgend genannten Gründen kann **keine Gewähr** dafür übernommen werden, dass die angebotenen Informationen auch die in Ihrer Einsatzumgebung bestehenden Fragestellungen und Probleme in jedem Fall abdecken:

- ✓ Rasante technologische Entwicklung im Bereich der Informationstechnologie.
- ✓ PC-basierte Computernetzwerke bestehen aus einer Vielzahl von Einzelkomponenten. Die im Einzelfall gegebene Zusammensetzung und mögliche Kompatibilitätsprobleme können nicht vorab bekannt sein.
- ✓ Sicherheit- und Datenschutzrisiken in Verbindung mit der Internetnutzung.
- ✓ Anzeigen des Dokumentes

2.5. Fachbegriffe

Ein Router kann aufgrund seiner zentralen Funktion für die Verbindung mit der "Außenwelt" vielleicht als "Herzstück" eines Netzwerkes bezeichnet werden. Ein Router verbindet ein in sich abgeschlossenes lokales Computernetzwerk (LAN) mit einem anderen, entfernten lokalen Computernetzwerk. Die Verbindung nutzt ein weiträumiges und allgemein zugängliches Datenverkehrssystem (WAN). Ein Verständnis für die Funktionsweise, die Vorteile und potentielle Probleme beim Einsatz eines Routers setzt ein grundlegendes Verständnis der Funktionsweise von Computern und Computernetzwerken voraus.

2.6. Abbildungen

Die in dieser Installationsanleitung abgebildeten Bildschirmfotos aus der Testinstallation wurden unter Microsoft Internet Explorer 6.0 mit Service Pack und aktiviertem Java Script erstellt. Wenn Sie einen anderen Webbrowser verwenden, wird das grafische Erscheinungsbild wahrscheinlich von den hier gezeigten Abbildungen abweichen.

Bitte beachten Sie, dass in vielen Fällen nicht das komplette Fenster des Internet Explorers abgebildet wird. Um überflüssige Bildinformationen zu vermeiden, wird in der Regel nur der Fensterbereich gezeigt, der die für die jeweilige Aktion relevanten visuellen Elemente enthält.

Auf Grund der Vereinheitlichung sind nur englische Screens in dieser Dokumentation abgebildet. Sie können sich selbstverständlich die Screens im Programm auf Deutsch anzeigen lassen. Nachdem Sie sich angemeldet haben, können Sie oberhalb der Menüleiste die Sprache wählen.

2.7. Druck dieser Anleitung

Diese Anleitung steht im Portable Document Format (PDF) zur Verfügung. Um das Dokument am Bildschirm darstellen oder ausdrucken zu können, benötigen Sie die kostenfrei erhältliche Software Acrobat Reader von Adobe. Für das Anzeigen dieses Dokumentes wird die Verwendung des Acrobat Readers in der Version 7 empfohlen. Sie können Acrobat Reader 7 von der Adobe Downloadseite (www.adobe.de) herunterladen.

Abbildungen und Formate in dieser Anleitung sind für den Ausdruck optimiert. Um das Dokument auszudrucken, klicken Sie im Hauptmenü des Acrobat Reader auf den Menüpunkt „Datei“ und „Drucken“.

2.8. Verwendete graphische Symbole

In dieser Anleitung werden die folgenden graphischen Zeichen verwendet, um Warnungen vor möglichen Gefahren und Risiken optisch besonders zu kennzeichnen. Die Zeichen entsprechen den Vorgaben der Berufsgenossenschaftlichen Vorschrift für Sicherheit und Gesundheit bei der Arbeit (BGV A8) von 2002.

Symbol	Bedeutung
	Warnung vor möglichen Gefahren und Risiken, die zu **Sachschäden und/oder Personenschäden führen können.**
	Warnung vor möglichen Gefahren und Risiken aufgrund **elektrischer Spannung.**
	Warnung vor Stolpergefahr.
	Verbot Die mit diesem Zeichen gekennzeichnete Aktion ist zur Vermeidung von Gefahren unbedingt zu unterlassen.
	Wichtiger Hinweis Bei Nichtbeachtung sind Probleme möglich oder wahrscheinlich.

3. Sicherheitshinweise

Dieses Kapitel enthält:

- ✓ Sicherheitshinweise und Vorsichtsmaßnahmen beim Betrieb dieses Produkts
- ✓ Warnungen vor potentiellen Schäden durch möglichen Fehlgebrauch

Bitte lesen Sie vor der Inbetriebnahme dieses Produkts die in diesem Kapitel dargestellten Sicherheitshinweise aufmerksam durch und beachten Sie die Ihnen zur Verfügung gestellten Informationen und Hinweise.

3.1. Bestimmungsgemäße Verwendung

Dieser Router wurde konzipiert für den Einsatz in kleineren und mittleren Büros und an Heimarbeitsplätzen. Eine verbreitete Bezeichnung für diesen Anwendungsbereich lautet "Small Office - Home Office" (SO-HO).

- ✓ Die Bereitstellung der Internetverbindung in einem Netzwerk schließt folgendes ein:
- ✓ Aufbau der Internetverbindung unter Nutzung eines externen (nicht im Lieferumfang enthaltenen) DSL-Modems oder Kabelmodems
- ✓ Verfügbarkeit der aufgebauten Internetverbindung für mehrere PCs im lokalen Netzwerk, z. B. in kleinen Büros.

Bei größeren Netzwerken muss zusätzlich ein Netzwerk-Switch eingesetzt werden. Verbinden Sie in diesem Fall einen Ethernet-Hub oder –Switch mit einem der LAN-Ports des Routers. So ist es auf einfache Weise möglich, so viele LAN-Ports an Ihrem Breitbandrouter bereitzustellen, wie Sie benötigen.

3.2. Bestimmungswidrige Verwendung

Folgende Verwendung des Routers gilt als nicht bestimmungsgemäß:

- ✓ Einsatz im Außenbereich oder in feuchten Räumen.
- ✓ Einsatz in hochsensiblen Umgebungen, die ein absolut fehlerfreies Funktionieren des IT-Systems erfordern und in denen ein technisches Versagen oder eine unangemessene oder missbräuchliche Anwendung zum Tod, zu Verletzungen oder anderen Schädigungen von Personen oder zu beträchtlichen Sach- oder Umweltschäden oder zu wirtschaftlichen bzw. finanziellen Schäden führen kann.

Das Produkt darf aus diesem Grund nicht in derartigen Verwendungszusammenhängen zum Einsatz gebracht werden. Beispiele für nicht vorgesehene Verwendungszusammenhänge sind:

- ✓ Krankenhäuser
- ✓ Flug- und Verkehrssicherung
- ✓ sensible Überwachungsanlagen

Eigenmächtige bauliche Veränderungen, An- oder Umbauten oder Reparaturversuche sind verboten. Eigenmächtige Manipulationen am Produkt oder am mitgelieferten Steckernetzteil können Gefahren für Sicherheit und Gesundheit einschließlich der Gefährdung unbeteiligter Personen hervorrufen!

3.3. Elektrische Spannung

Achten sie darauf, dass keine Flüssigkeiten oder Gegenstände (z. B. Büroklammern) in das Gehäuse dieses Produkts gelangen! Sonst besteht Gefahr durch elektrischen Schlag und Kurzschluss.

3.4. Steckernetzteil

- ✓ Verwenden Sie ausschließlich das mitgelieferte Netzteil. Bei Verwendung eines Netzteils mit abweichenden Ausgangswerten kann der Router beschädigt werden.
- ✓ Der Spannungswert der Stromversorgung am Einsatzort muss innerhalb des zulässigen Bereichs (100-240 Volt, 50-60 Hz) liegen. Dieser ist oben auf dem Steckernetzteil angegeben.
- ✓ Um Gefährdungen durch elektrischen Strom zu vermeiden, darf das Steckernetzteil ausschließlich an eine ordnungsgemäß geerdete Steckdose (Schukosteckdose) angeschlossen werden. Verwenden sie keine Adapterstecker.

- ✓ Das Steckernetzteil darf durch den Benutzer auf keinen Fall geöffnet werden. Bitte versuchen Sie auf keinen Fall, das Steckernetzteil selbst zu reparieren. **Es besteht Gefahr durch Stromschlag!**
  Bei einem Defekt des Steckernetzteils oder der Kabelzuleitung kontaktieren Sie bitte zur Beschaffung eines Ersatznetzteils Ihren Händler oder nutzen Sie die Hotline des Herstellers.

- ✓ Spannungsführende Steckerkontakte oder Buchsen auf keinen Fall direkt oder mit spitzen, metallischen oder feuchten Gegenständen berühren! **Es besteht Gefahr durch Stromschlag!**

- ✓ Das Steckernetzteil darf nicht mehr verwendet werden, wenn Beschädigungen an der Kabeleinführung, dem Knickschutz oder der Isolierung der beweglichen Anschlussleitung vorliegen! **Es besteht Gefahr durch Stromschlag!**
- ✓ Nie am beweglichen Anschlusskabel des Steckernetzteils ziehen!

3.5. Blitzschlag und Überspannung

Ein Blitzschlag in der näheren Umgebung kann zu Schäden an den elektronischen Bauteilen und Überspannung führen. Schädigende Spannungsspitzen können sowohl im 230 Volt-Stromnetz als auch im Telefonleitungsnetz auftreten.

- ✓ Stellen Sie während eines Gewitters keine neuen Kabelverbindungen her und berühren Sie während des Gewitters keine Datenübertragungsleitungen.
- ✓ Trennen Sie vor Beginn eines Gewitters das Steckernetzteil des Produkts vom Stromnetz.
- ✓ Trennen Sie vor einem Gewitter auch die Kabelverbindungen zum Telefonleitungsnetz (Verbindung zwischen DSL-Modem und Splitter).

3.6. Aufstellort und Umgebungsbedingungen

Der Aufstellort des Produkts muss die folgenden Bedingungen erfüllen:

- ✓ Die mit dem Produkt verbundenen Kabel sind so zu verlegen, dass keine Stolpergefahr entsteht und versehentliches Belasten der Kabel, Hängenbleiben etc. ausgeschlossen sind.
- ✓ Die Umgebung muss trocken sein.
- ✓ Stellen Sie das Produkt so auf, dass nicht versehentlich Flüssigkeiten mit dem Produkt in Kontakt kommen können, z.B. durch Umkippen von Getränken, Blumenvasen etc.
- ✓ Positionieren Sie das Produkt außerhalb der Reichweite von Kindern oder Haustieren.
- ✓ Stellen Sie den Router auf einem stabilen Untergrund auf.

3.7. Temperatur

- ✓ Stellen Sie das Produkt so auf, dass gute Belüftung von allen Seiten gewährleistet ist. Insbesondere ist darauf zu achten, dass die für die Gehäusebelüftung vorhandenen Lüftungsschlitze oder Gehäuseaussparungen nicht blockiert werden. Vermeiden Sie die Platzierung zwischen anderen Objekten.
- ✓ Schützen Sie das Produkt vor direkter Sonneneinstrahlung. Vermeiden Sie die Aufstellung in unmittelbarer Nähe eines Fensters.
- ✓ Stellen Sie das Produkt nicht auf elektronische Produkte oder andere Objekte, die sich erwärmen.
- ✓ Eine überhöhte Betriebstemperatur führt mit hoher Wahrscheinlichkeit zu vorübergehenden oder sogar anhaltenden Funktionsstörungen. Nach einer erwärmungsbedingten Funktionsstörung sollten Sie das Produkt für einige Minuten vom Stromnetz trennen.

3.8. Feuchtigkeit

- ✓ Berühren Sie das Steckernetzteil oder das Produkt niemals mit nassen oder feuchten Händen.
- ✓ Router und Steckernetzteil dürfen niemals mit Wasser oder anderen Flüssigkeiten in Kontakt kommen, nass oder feucht werden.
- ✓ Das Produkt darf nicht betrieben werden, wenn die Luftfeuchtigkeit den im Datenblatt angegebenen zulässigen Höchstwert übersteigt.
- ✓ Das Produkt darf nicht in feuchten Bereichen im Innenraum eingesetzt werden wie z. B. Badezimmern oder Küchen, in feuchten Kellerräumen oder in Kellerräumen ohne eigene Entwässerung.
- ✓ Stellen Sie das Produkt nicht in unmittelbarer Nähe eines Fensters auf. Ferner kann das Produkt bei geöffnetem oder gekipptem Fenster (bzw. Oberlicht) im Falle von plötzlich einsetzendem starken Regen im ungünstigen Fall nass werden, was unbedingt zu vermeiden ist.

3.9. Vorsichtsmaßnahmen zum Schutz von Kindern

Stellen Sie das Produkt so auf, dass es für Kinder nicht erreichbar ist.

3.10. Zielgruppe und Anforderungen an den Benutzer

Dieses Produkt ist für den Einsatz durch Computernutzer ausgelegt, die über hinreichende Fachkenntnis im Umgang mit dem PC verfügen und die Beachtung der Sicherheitshinweise gewährleisten können.

Für die Inbetriebnahme und Konfiguration / Wartung dieses Produkts sind die folgenden Voraussetzungen und Kenntnisse erforderlich:

- ✓ Sichere und verantwortliche Handhabung von elektrischen Produkten und Telekommunikationseinrichtungen.
- ✓ Kenntnisse über Ihr Betriebssystem und TCP-IP-Netzwerke.

Wenn diese Voraussetzungen nicht erfüllt sind, sollte die Inbetriebnahme und Konfiguration / Wartung durch Fachpersonal ausgeführt werden, um Risiken und mögliche Schäden infolge Fehlbedienung oder Fehlkonfiguration zu vermeiden.

Dieses Produkt ist nicht speziell ausgelegt und vorbereitet für Einsatz und Verwendung durch

- ✓ Menschen mit Behinderungen
- ✓ Senioren
- ✓ Kinder

Die Nutzung dieses Produkts, z. B. für die Anbindung an das Internet, ist für die o. g. Verwendergruppen deswegen nur unter der Voraussetzung möglich, dass Unterstützung und falls notwendig Beaufsichtigung durch eine sachkundige Person erfolgt.

3.11. Potentielle finanzielle Schadensrisiken

3.11.1. Ungewollte Online-Verbindungsgebühren

Wenn die Gebühren für ihre Internetverbindung in Abhängigkeit von der Verbindungsdauer berechnet werden, ist es sehr wichtig, dass Sie den Bereich ihres Routers und den Status der Internetverbindung überwachen, um das unbeabsichtigte Entstehen von Verbindungskosten zu vermeiden.

Um sicherzugehen, dass keine ungewollten Verbindungsgebühren anfallen, sollten Sie die Internetverbindung manuell aufbauen und beenden.

Digital Data Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungsgebühren und Schäden, die durch unbeaufsichtigten Betrieb des Routers entstanden sind.

3.11.2. Ausfall des IT-Systems

Bereits in kleinen Netzwerken kann der Ausfall einer einzigen Komponente, insbesondere an zentralen Knotenpunkten des Systems, zu einem Ausfall des gesamten Systems führen.

Wenn Sie Ihren VoIP-Router sowohl für die Internetanbindung (als Gateway) als auch als zentralen Knotenpunkt für Ihren lokalen Netzwerkverkehr im LAN einsetzen, spielt er in Ihrem Netzwerk die Rolle eines zentralen Kontenpunktes. In diesem Fall bewirkt ein Ausfall des Routers, dass sowohl die Internetanbindung als auch die im lokalen Netzwerk gespeicherten Daten und Geräte (z.B. Drucker) vorübergehend nicht zur Verfügung stehen.

Neben technischem Versagen und höherer Gewalt (z.B. Überspannung nach einem Blitzeinschlag) sind es häufig Bedienungsfehler bzw. menschliches Fehlverhalten, die für den Ausfall einer IT-Komponente verantwortlich sind.

3.11.3. Ausfall der Internetverbindung

Beispiel: Ausfall/Störung der DSL-Verbindungsstelle

Wenn Sie auf absolut ausfallsicheres Funktionieren Ihres IT-Systems angewiesen sind, ist es zu empfehlen, für den Störungsfall die Möglichkeit der Anbindung an das Internet über ISDN (oder einen analogen Telefonanschluss via Modem) bereitzustellen. Für die Internetanbindung kleiner Netzwerke kann dies am einfachsten mit einem ISDN-Router gelöst werden, der bereits im Vorfeld für den Verbindungsaufbau im Notfall entsprechend vorbereitet wird. Alternativ sollte, wenn absolute Ausfallsicherheit der Internetanbindung gefordert ist, auf Router mit ISDN Backup Modul, das bei DSL-Verbindungsproblemen automatisch einspringt, zurückgegriffen werden.

3.11.4. Vorsicht bei Firmware-Upgrades

Beachten Sie die Hinweise zu Vorgehen und Risiken bei einem Upgrade der Firmware!

3.11.5. Notwendige Maßnahmen zum Schutz Ihres Netzwerkes

Im Rahmen von Inbetriebnahme des Routers und Ersteinrichtung der Internetverbindung sind die folgenden Maßnahmen zum Schutz Ihres Netzwerkes und Ihrer Daten vor unbefugtem Eindringen von außen unbedingt durchzuführen:

- ✓ Sicheres Administrator-Passwort setzen
- ✓ Universal Plug'n Play und Fernkonfiguration abschalten
- ✓ Zugriffskontrolle aktivieren (z.B. MAC-Filter)

4. Technische Details

4.1. LEDs an der Vorderseite

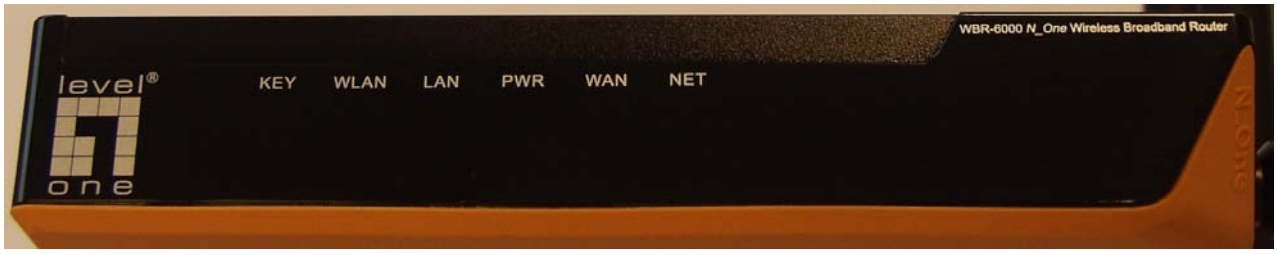


Abb. 3 Vorderseite des Geräts

KEY	**Ein**- WLAN-Sicherheit ist aktiv.
	Aus- WLAN-Sicherheit ist inaktiv.
WLAN	**Ein** - WLAN ist aktiv.
	Aus - Es ist keine WLAN-Verbindung vorhanden.
	Blinkt - Es werden Daten über den Wireless Access Point gesendet oder empfangen. Dabei kann es sich um „Netzwerkverkehr“ oder Anwenderdaten handeln.
LAN	**Ein** - Der entsprechende LAN (Hub)-Port ist aktiv.
	Aus - Es gibt keine aktive Verbindung am entsprechenden LAN (Hub)-Port.
	Blinkt - Daten werden über den LAN (Hub)-Port gesendet oder empfangen.
PWR	**Ein** - Stromversorgung ist in Ordnung.
	Aus - Stromversorgung ist unterbrochen.
	Blinkt - Die LED blinkt beim Start und während eines Firmware-Upgrades.
WAN	**Ein** - Verbindung zum Modem am WAN-Port wurde hergestellt.
	Blinkt - Daten werden über den WAN-Port gesendet oder empfangen.
NET	**Ein** - Eine Internetverbindung ist verfügbar.
	Ein - Es ist keine Internetverbindung verfügbar.
	Blinkt - Daten werden über die ADSL-Verbindung gesendet oder empfangen.

4.2. Rückseite des Geräts

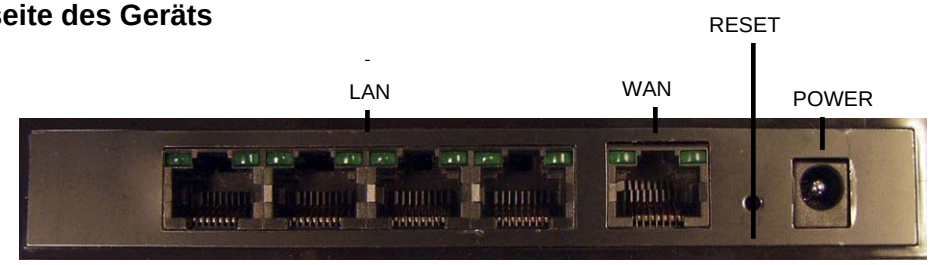


Abb. 4 Rückseite des Geräts

10/100BaseT LAN-Verbindungen	Verwenden Sie handelsübliche LAN-Kabel (RJ45-Verbinder), um Ihre PCs an diese Ports anzuschließen. **Hinweis:** Jeder LAN-Port auf dem WLAN-Breitbandrouter funktioniert im Bedarfsfall automatisch als „Uplink"-Port. Verbinden Sie einen Port mit einem normalen Port am anderen Hub mittels eines handelsüblichen LAN-Kabels.
WAN-Port (10/100BaseT)	Schließen Sie hier das DSL- oder Kabelmodem an. Wenn ein Kabel mitgeliefert wurde, benutzen Sie dieses. Andernfalls verwenden Sie bitte ein handelsübliches LAN-Kabel.
Reset-Taste	Diese Taste hat zwei (2) Funktionen: • **Neustart**. Halten Sie die Reset-Taste 5 Sekunden lang gedrückt. Lassen Sie dann die Taste los und warten Sie bis der WLAN-Breitbandrouter einen Neustart durchgeführt hat. • **Alle Daten löschen**. Die Reset-Taste kann auch genutzt werden, um ALLE Daten zu löschen und ALLE werkseitig vorgegebenen Einstellungen wiederherzustellen. Um alle Daten zu löschen und die werkseitig vorgegebenen Werte wiederherzustellen, gehen Sie bitte wie folgt vor: ● Schalten Sie die Stromversorgung ein und halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Lassen Sie die Taste dann wieder los. Der WLAN-Breitbandrouter wird neu gestartet und verwendet nun die werkseitig voreingestellten Werte.
Power	Schließen Sie hier das mitgelieferten Netzteil an.

5. Installation

Dieses Kapitel beschreibt die Installation des WLAN-Breitbandrouters.

5.1. Voraussetzungen

- Verwenden Sie handelsübliche 10/100BaseT-Netzwerkkabel (UTP) mit RJ45-Anschluss.
- Das TCP/IP-Protokoll muss auf allen PCs installiert sein.
- Für den Internetzugang sind ein Internet-Account bei einem Internet-Service-Provider sowie ein DSL-Anschluss erforderlich.
- Alle eingesetzten Geräte müssen den Standards IEEE 802.11g, IEEE 802.11b oder dem Entwurf IEEE 802.11n entsprechen.

5.2. Vorgehensweise

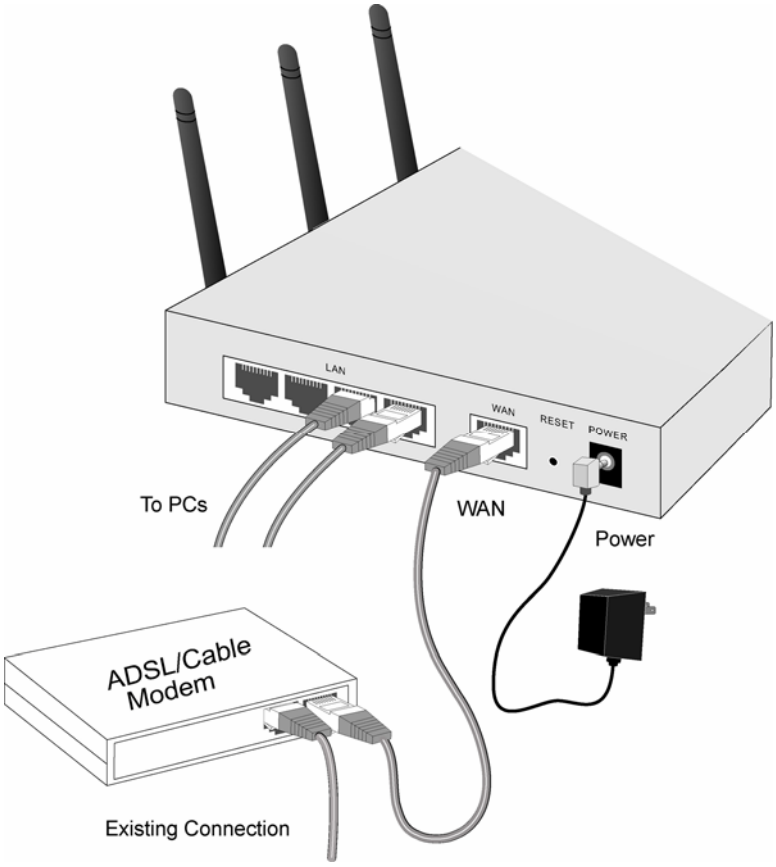


Abb. 5 Installationsdiagramm

1. Wahl des Standorts

Wählen Sie einen geeigneten Standort im Netzwerk für die Installation des WLAN-Breitbandrouters.

Für optimalen Funkempfang und optimale Leistung sollte der WLAN-Breitbandrouter an einem zentralen Ort aufgestellt werden, an dem sich möglichst wenige Hindernisse zwischen dem WLAN-Breitbandrouter und den PCs befinden.
Beim Gebrauch von mehreren Access Points sollten benachbarte Access Points auf unterschiedliche Kanäle eingestellt werden.

2. Anschluss der LAN-Kabel

Verwenden Sie handelsübliche LAN-Kabel, um die PCs an die Ports des Switching Hubs am WLAN-Breitbandrouter anzuschließen. 10BaseT- und 100BaseT-Verbindungen können gleichzeitig verwendet werden.

Falls erforderlich, kann ein beliebiger Port mit einem normalen Port eines anderen Hubs verbunden werden. Verwenden Sie auch hier ein handelsübliches LAN-Kabel. Jeder LAN-Port auf dem WLAN-Breitbandrouter funktioniert im Bedarfsfall automatisch als „Uplink“-Port.

3. Anschluss des WAN-Kabels

Verbinden Sie das DSL- oder Kabelmodem mit dem WAN-Port auf dem WLAN-Breitbandrouter. Verwenden Sie das Kabel, das mit Ihrem DSL- / Kabelmodem mitgeliefert wurde. Sollte kein Kabel mitgeliefert worden sein, benutzen Sie bitte ein handelsübliches Kabel.

4. Inbetriebnahme

Verbinden Sie das mitgelieferte Netzteil mit dem WLAN-Breitbandrouter. Verwenden Sie ausschließlich das mitgelieferte Netzteil. Die Verwendung eines anderen Netzteils kann zu Hardwareschäden führen.

5. Prüfen der LEDs

- Die Netz-LED *PWR* sollte leuchten.
- Für jede LAN-Verbindung (PC) sollte eine LAN-LED leuchten (vorausgesetzt, der PC ist ebenfall eingeschaltet).
- Die *WLAN*-LED sollte leuchten, wenn WLAN-Clients verbunden sind.
- Die *WAN*-LED sollte leuchten, wenn das DSL- oder Kabelmodem eingeschaltet ist.
- Die *Net*-LED leuchtet möglicherweise nicht. Nach der Konfiguration im Setup-Assistenten sollte sie leuchten.

Für weitere Informationen lesen Sie bitte *LEDs an der Vorderseite in* Kapitel 4.

6. Setup

Dieses Kapitel befasst sich mit Einzelheiten bezüglich der Einstellung des WLAN-Breitbandrouters.

6.1. Übersicht

In diesem Kapitel wird das Setup für die folgenden Parameter beschrieben:

- Internetzugang
- LAN-Konfiguration
- WLAN-Setup
- Zuweisen eines Passworts zum Schutz der Konfigurationsdaten

PCs in Ihrem LAN müssen eventuell ebenfalls konfiguriert werden. Weitere Informationen hierzu finden Sie in *Kapitel 7 - PC-Konfiguration*.

Je nachdem, welche Eigenschaften und Funktionen des WLAN-Breitbandrouters Sie nutzen möchten, müssen unter Umständen weitere Konfigurationen vorgenommen werden. Die folgende Tabelle enthält detaillierte Anweisungen bezüglich der benötigten Funktionen.

Vorgang:	**Kapitel:**
Konfigurieren von PCs in Ihrem LAN.	Kapitel 7: PC-Konfiguration
Überprüfen des WLAN-Breitbandrouter-Betriebs und -Status.	Kapitel 8: Betrieb und Status
Verwendung einer der nachfolgenden erweiterten Funktionen: • Internet (DMZ, URL-Filter) • Zugriffskontrolle • Dynamisches DNS • Firewall-Regeln • Firewall-Dienste • Virtuelle Server • Optionen • Zeitpläne	Kapitel 9: Erweiterte Funktionen

Verwendung einer der nachfolgenden Funktionen für die Verwaltungskonfiguration: • PC-Datenbank • Diagnose • Konfigurationsdatei • Logs • Externe Verwaltung • Firmware-Upgrade	Kapitel 10 Erweiterte Verwaltung

6.2. Konfigurationsprogramm

Der WLAN-Breitbandrouter beinhaltet einen HTTP-Server. Dadurch haben Sie die Möglichkeit, mit Ihrem Web-Browser auf diesen zuzugreifen und ihn zu konfigurieren.
Ihr Browser muss dazu jedoch JavaScript unterstützen.

Das Konfigurationsprogramm wurde auf folgenden Browsern getestet:

- Netscape 7.1 oder neuere Version
- Mozilla 1.6 oder neuere Version
- Internet Explorer V5.5 oder neuere Version

6.2.1. Vorbereitung

Vor der Konfiguration des WLAN-Breitbandrouters stellen Sie bitte Folgendes sicher:

- Ihr PC ist in der Lage, eine physische Verbindung zum WLAN-Breitbandrouter herzustellen. Der PC und der WLAN-Breitbandrouter sind direkt miteinander verbunden (über die Hub-Ports auf demWLAN-Breitbandrouter) oder befinden sich auf demselben LAN-Segment.
- Der WLAN-Breitbandrouter ist installiert und eingeschaltet.
- Falls die Standard-IP-Adresse des WLAN-Breitbandrouters (192.168.0.1) bereits durch ein anderes Gerät genutzt wird, muss dieses Gerät so lange ausgeschaltet sein, bis dem WLAN-Breitbandrouter während der Konfiguration eine neue IP-Adresse zugeordnet wurde.

6.2.2. Verwendung des Web-Browsers

Um eine Verbindung vom PC zum WLAN-Breitbandrouter herzustellen, gehen Sie bitte wie folgt vor:

1. Fahren Sie Ihren PC nach der Installation des WLAN-Breitbandrouters in Ihrem LAN hoch. Falls Ihr PC bereits eingeschaltet ist, führen Sie einen Neustart durch.
2. Starten Sie Ihren Web-Browser.
3. Geben Sie in das *Addressenfeld* „HTTP://“ gefolgt von der IP-Adresse des WLAN-Breitbandrouters ein. Im folgenden Beispiel wird dazu die Standard-IP-Adresse des WLAN-Breitbandrouters verwendet:

   HTTP://192.168.0.1
4. Geben Sie den folgenden Benutzernamen und Passwort ein:
   - Benutzername admin
   - Passwort password

6.2.3. Verbindungsaufbau nicht möglich

Falls der WLAN-Breitbandrouter keine Verbindung herstellen kann, überprüfen Sie die folgenden Punkte:

- Der WLAN-Breitbandrouter ist korrekt installiert, die LAN-Verbindung ist OK und das Gerät ist eingeschaltet. Sie können die Verbindung testen, indem Sie den „Ping“-Befehl benutzen:
- Öffnen Sie das MS-DOS-Fenster oder das Befehlseingabefenster.
- Geben Sie den folgenden Befehl ein:

  ping 192.168.0.1

Wenn Sie keine Antwort erhalten, funktioniert entweder die Verbindung nicht oder die IP-Adresse Ihres PCs ist nicht kompatibel mit der des WLAN-Breitbandrouters (siehe nächster Punkt.)

- Falls Ihr PC eine feste IP-Adresse verwendet, muss diese im Bereich zwischen 192.168.0.2 und 192.168.0.254 liegen, um mit der IP-Adresse des WLAN-Breitbandrouters (192.168.0.1) kompatibel zu sein. Darüber hinaus muss die Netzwerkmaske auf 255.255.255.0 eingestellt sein. Weitere Informationen zur Überprüfung der TCP/IP-Einstellungen Ihres PCs finden Sie in Kapitel 7 - PC-Konfiguration.
- Stellen Sie sicher, dass sich Ihr PC und der WLAN-Breitbandrouter im selben Netzwerksegment befinden. (Wenn Sie keinen Router verwenden, sollte dies der Fall sein.)

Stellen Sie sicher, dass Sie die drahtgebundene LAN-Schnittstelle verwenden. Die WLAN-Schnittstelle kann nur dann verwendet werden, wenn deren Konfiguraiton mit den Einstellungen des PCs übereinstimmt

6.3. Einrichtungsassistent

Starten Sie den Einrichtungsassistenten beim ersten Verbindungsaufbau zum WLAN-Router.

1. Führen Sie alle Anweisungen des Assistenten Schritt für Schritt durch.

- Ihnen muss der Internetverbindungsservice, der von Ihrem Internet-Service-Provider verwendet wird, bekannt sein. Prüfen Sie die Daten, die Ihnen von Ihrem Internet-Service-Provider mitgeteilt wurden.
- Die gebräuchlichsten Verbindungsarten sind in der nachfolgenden Tabelle aufgeführt.

2. Führen Sie in der letzten Bildschirmanzeige des Assistenten den Verbindungstest durch und überprüfen Sie, ob die Internetverbindung hergestellt werden kann.
3. Wenn der Verbindungstest fehlschlägt, gehen Sie wie folgt vor:

- Überprüfen Sie Ihre Daten, das Kabel- / DSL-Modem und alle Verbindungen.
- Überprüfen Sie, ob Sie alle Daten richtig eingegeben haben.
- Wenn Sie ein Kabelmodem verwenden, könnte Ihr Internet-Service-Provider die MAC-Adresse (physische Adresse) Ihres PCs aufgezeichnet haben. Starten Sie den Assistenten und verwenden Sie die Schaltfläche „Klone MAC-Adresse“ in der Bildschirmanzeige *Kabelmodem*, um die MAC-Adresse von Ihrem PC auf den WLAN-Router zu kopieren.

6.3.1. Gebräuchliche Verbindungsarten

Kabelmodems

Typ	Details	Erforderliche ISP-Daten
Dynamische IP-Adresse	Ihre IP-Adresse wird Ihnen automatisch beim Verbindungsaufbau zu Ihrem ISP zugeordnet.	Für gewöhnlich keine. Einige Internet-Service-Provider verlangen möglicherweise die Verwendung eines bestimmten Hostnamens, Domainnamens oder einer (physischen) MAC-Adresse.
Statische (feste) IP-Adresse	Ihr ISP weist Ihnen eine permanente IP-Adresse zu.	IP-Adresse, die Ihnen zugewiesen wurde. Außerdem ist es möglich, dass einige Internet-Service-Provider die Verwendung eines bestimmten Hostnamens, Domainnamens oder einer (physischen) MAC-Adresse verlangen.

DSL-Modems

Typ	Details	Erforderliche ISP-Daten
Dynamische IP-Adresse	Ihre IP-Adresse wird Ihnen automatisch beim Verbindungsaufbau zu Ihrem ISP zugeordnet.	Keine.
Statische (feste) IP-Adresse	Ihr ISP weist Ihnen eine permanente IP-Adresse zu.	IP-Adresse, die Ihnen zugewiesen wurde.
PPPoE	Verbindungsaufbau zum ISP nur nach Bedarf. Die IP-Adresse wird normalerweise automatisch zugewiesen.	Benutzername und Passwort.
PPTP	PPTP wird hauptsächlich in Europa verwendet. Verbindungsaufbau zum ISP nur nach Bedarf. Die IP-Adresse wird gewöhnlich automatisch zugeordnet, kann aber auch statisch (fest) sein.	•

Andere Modems (z. B. Breitband WLAN)

Typ	Details	Erforderliche ISP-Daten
Dynamische IP-Adresse	Ihre IP-Adresse wird Ihnen automatisch beim Verbindungsaufbau zu Ihrem ISP zugeordnet.	Keine.
Statische (feste) IP-Adresse	Ihr ISP weist Ihnen eine permanente IP-Adresse zu.	IP-Adresse, die Ihnen zugewiesen wurde.

Big Pond (Australien)

Für diese Verbindungsmethode sind die folgenden Daten erforderlich:

- Benutzername
- Passwort
- IP-Adresse des Big Pond Servers

SingTel RAS

Für diese Verbindungsmethode sind die folgenden Daten erforderlich:

- Benutzername
- Passwort
- RAS-Plan

6.4. Bildschirmanzeige Home

Bei Zugriff auf den WLAN-Breitbandrouter wird die Bildschirmanzeige *Home* eingeblendet. Dafür müssen Sie zunächst den **Einrichtungsassistenten** durchgeführt haben. Ein Beispielbildschirm ist unten abgebildet.

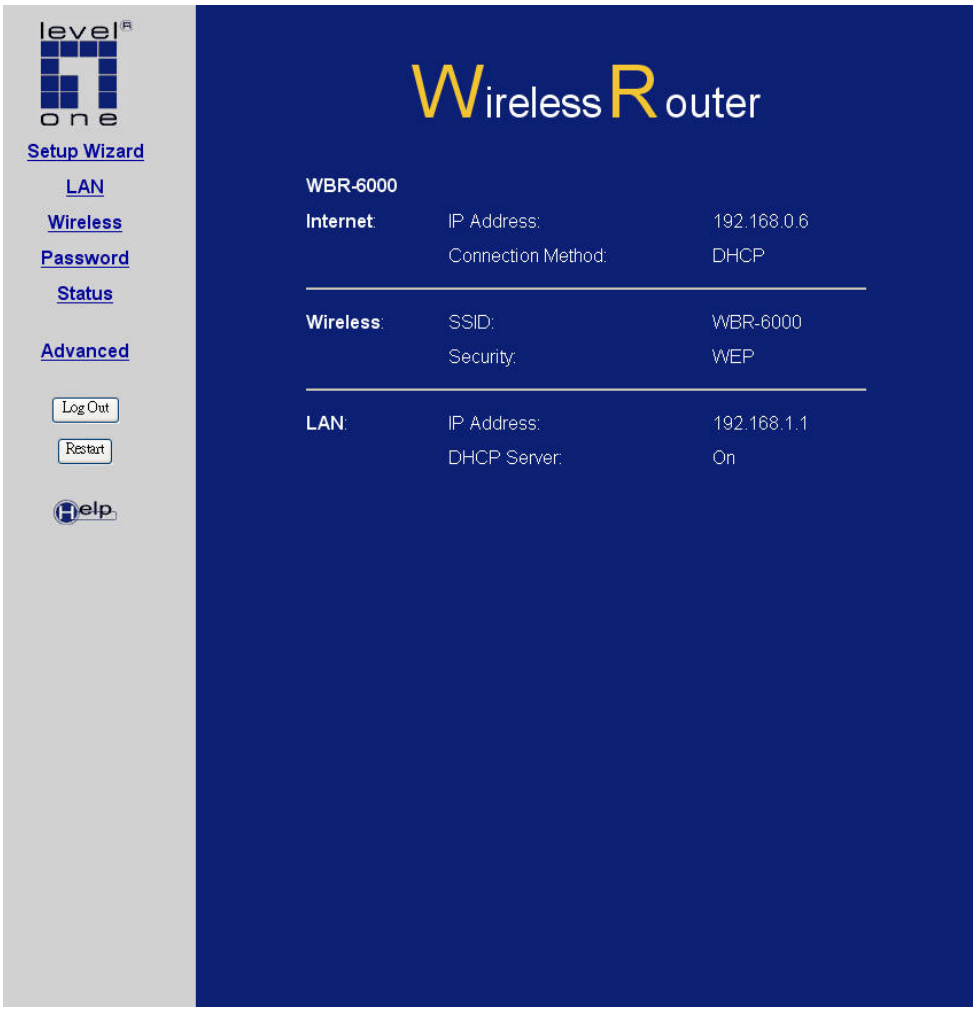


Abb. 6 Bildschirmanzeige Home

6.4.1. Hauptmenü

Das Hauptmenü im linken Bereich des Fensters enthält Links zu den am häufigsten verwendeten Bildschirmanzeigen.

Darüber hinaus sind im Hauptmenü zwei Schaltflächen vorhanden:

- **Log Out** - Klicken Sie auf diese Schaltfläche, um sich abzumelden.
- **Restart** - Klicken Sie auf diese Schaltfläche, um den WLAN-Breitbandrouter neu zu starten. Beachten Sie, dass bei einem Neustart des Routers alle bestehenden Verbindungen zum oder über den Router abgebrochen werden.

6.4.2. Navigation und Dateneingabe

- Verwenden Sie zur Navigation entweder die Menüleiste auf der linken Seite des Bildschirms oder klicken Sie in Ihrem Browser auf „Zurück“.
- Wenn Sie zu einem anderen Bildschirm wechseln, ohne zuvor auf „Save“ zu klicken, werden von Ihnen vorgenommene Änderungen NICHT übernommen. Um die geänderten Daten zu übernehmen, müssen Sie auf „Save“ klicken, bevor Sie in einen anderen Bildschirm wechseln.

Auf jedem Bildschirm kann durch Klicken auf „Help“ ein Hilfetext für den entsprechenden Bildschirm aufgerufen werden.

6.5. Bildschirmanzeige LAN

Über den Link *LAN* im Hauptmenü gelangen Sie zur Bildschirmanzeige LAN. Ein Beispielbildschirm ist unten abgebildet.

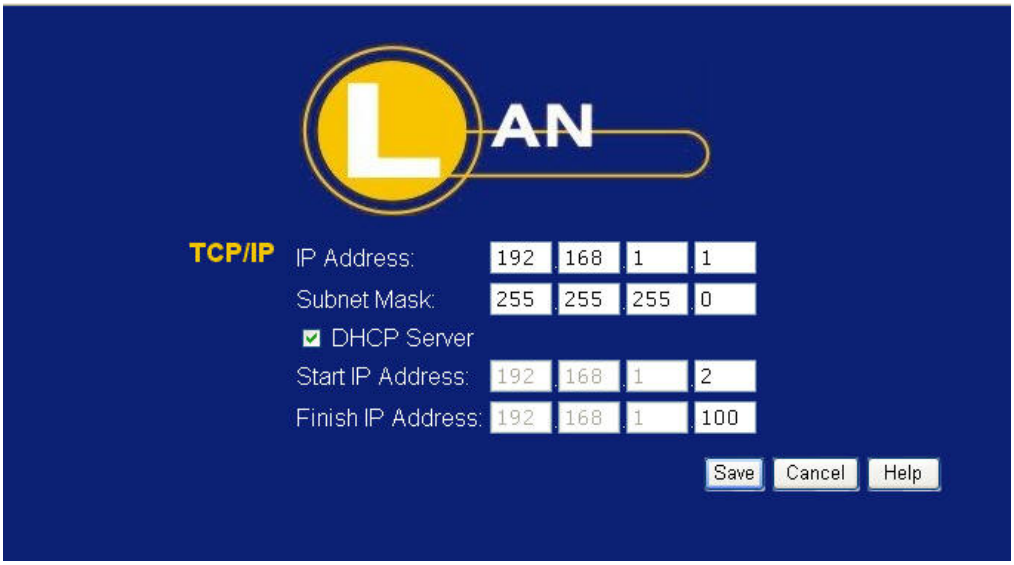


Abb. 7 Bildschirmanzeige LAN

6.5.1. Daten - Bildschirmanzeige LAN

TCP/IP	
IP Address	IP-Adresse für den WLAN-Breitbandrouter, wie vom LAN aus gesehen. Verwenden Sie die Standardeinstellung, sofern diese IP-Adresse noch nicht von einem anderen Gerät verwendet wird und sie für den IP-Bereich, den Ihr Netzwerk verwendet, geeignet ist. Ist Letzteres nicht der Fall, geben Sie eine unbenutzte IP-Adresse ein, die innerhalb des Bereichs liegt, den Ihr LAN verwendet.
Subnet Mask	Kleine Netzwerke (Klasse „C“) verwenden die Standardeinstellung 255.255.255.0. Für andere Netzwerke benutzen Sie bitte die Subnetzmaske für das LAN-Segment, an das der WLAN-Breitbandrouter angeschlossen ist (derselbe Wert wie bei den PCs in diesem LAN-Segment).
DHCP Server	• Wenn aktiviert, weist der WLAN-Breitbandrouter den PCs (DHCP-Clients) beim Hochfahren IP-Adressen zu. Diese Funktion ist standardmäßig aktiviert und wird empfohlen. • Wenn Sie bereits einen DHCP-Server verwenden, muss diese Einstellung deaktiviert und der existierende DHCP-Server erneut konfiguriert werden, um den WLAN-Breitbandrouter als Standard-Gateway verwenden zu können. Nähere Information hierzu entnehmen Sie bitte dem nächsten Abschnitt. • Die Felder **Start IP Address** und **Finish IP Address** geben die Werte vor, die der DHCP-Server bei Zuweisung von IP-Adressen an DHCP-Clients verwendet. Dieser Bereich bestimmt auch die Anzahl der unterstützten DHCP-Clients. Im folgenden Abschnitt erfahren Sie Näheres über die Verwendung von DHCP.

6.5.2. DHCP

6.5.2.1. Funktionen des DHCP

Ein **DHCP-Server** (Dynamic Host Configuration Protocol) weist einem **DHCP-Client** (PC oder anderes Gerät) auf Anfrage eine gültige IP-Adresse zu.

- Die Clientanfrage wird ausgegeben, wenn das Clientgerät startet.
- Der DHCP-Server liefert dem Client die *Gateway*- und *DNS*-Adressen und weist ihm eine IP-Adresse zu.
- Der WLAN-Breitbandrouter kann ebenfalls als **DHCP-Server** fungieren.
- Windows und andere Nicht-Server-Versionen von Windows fungieren als DHCP-**Client**. Hierbei handelt es sich um die Standardeinstellung von Windows für TCP/IP-Netzwerkprotokolle. Allerdings verwendet Windows anstelle von „DHCP-Client“ die Bezeichnung *IP-Adresse automatisch beziehen*.
- Es ist NICHT gestattet, dass sich zwei oder mehrere DHCP-Server im selben LAN-Segment befinden. (Wenn sich in Ihrem LAN nur ein Router befindet, bedeutet dies, dass nur ein DHCP-Server an Ihr LAN angeschlossen sein muss.)

6.5.2.2. Verwendung des DHCP-Servers des WLAN-Breitbandrouters

Hierbei handelt es sich um die Standardeinstellung. Die DHCP-Servereinstellungen befinden sich in der Bildschirmanzeige ***LAN***. Auf diesem Bildschirm können Sie folgende Einstellungen vornehmen:

- Aktivieren oder Deaktivieren der DHCP-*Server*-Funktion des WLAN-Breitbandrouters.
- Festlegen des IP-Adressenbereichs, der den PCs über die DHCP-Server-Funktion zugeordnet wird.

Mit DHCP können Sie Geräten statische IP-Adressen zuordnen, vorausgesetzt, dass diese statischen IP-Adressen sich NICHT innerhalb des Bereichs befinden, der vom DHCP-Server genutzt wird.

6.5.2.3. Verwendung eines weiteren DHCP-Servers

Pro LAN-Segment kann nur ein DHCP-Server verwendet werden. Sollten Sie einen anderen DHCP-Server verwenden wollen als den WLAN-Breitbandrouter, gehen Sie bitte wir folgt vor:

- Deaktivieren Sie die Funktion „DHCP-Server“ im WLAN-Breitbandrouter. Diese Einstellung befindet sich in der Bildschirmanzeige LAN.
- Konfigurieren Sie den DHCP-Server so, dass die IP-Adresse des WLAN-Breitbandrouters als *Standard-Gateway* festgelegt ist.

6.5.2.4. Konfiguration Ihrer PCs für die Verwendung von DHCP

Bei allen Nicht-Server-Versionen von Windows ist das TCP/IP-Protokoll standardmäßig für die Verwendung von DHCP eingestellt.

Die Vorgehensweise zur Überprüfung dieser Einstellungen finden Sie in *Kapitel 9 – Erweiterte Funkitionen*.

6.5.3. Bildschirmanzeige Wireless

Die Einstellungen des WLAN-Breitbandrouters müssen mit denen der übrigen WLAN-Stationen übereinstimmen.

Hinweis: Der WLAN-Breitbandrouter ist standardmäßig so eingestellt, dass er die Verbindunsstandards 802.11b, 802.11g und den Entwurf 802.11n verwenden kann. Hierfür sind keine weiteren Einstellungen erforderlich.

Um Änderungen an den Standardeinstellungen des WLAN-Breitbandrouters für die Funktion Wireless Access Point vorzunehmen, verwenden Sie den Link *Wireless* im Hauptmenü, um zur Bildschirmanzeige ***Wireless*** zu gelangen. Ein Beispielbildschirm ist unten abgebildet.

Abb. 8 Bildschirmanzeige Wireless

Daten - Bildschirmanzeige Wireless

Identification	
Region	Wählen Sie für Ihren Standort die richtige Domain aus. Es obliegt Ihrer Verantwortung, dafür zu sorgen, dass: • der WLAN-Breitbandrouter nur in Regionen verwendet wird, für die er zugelassen ist. • Sie durch Auswahl der korrekten Region sicherstellen, dass nur legale Kanäle dieser Region genutzt werden können.
Station Name	Entspricht dem „Gerätenamen“ des WLAN-Breitbandrouters.
SSID	Der Name des Netzwerks. • Wenn Sie ein ESS (Extended Service Set – Erweiterungsgerät mit mehreren Access Points) verwenden, wird diese ID als SSID bzw. ESSID (Extended Service Set Identifier) bezeichnet. • Um kommunizieren zu können, sollten alle WLAN-Stationen die gleiche SSID / ESSID verwenden.
Options	
Modus	Wählen Sie die gewünschte Option: • **Off** - Deaktiviert die Wireless-AP-Funktion. • **802.11b** - Nur 802.11b-Verbindungen sind verfügbar. 802.11g Wireless-Stationen können den WLAN-Breitbandrouter nur dann nutzen, wenn Sie vollständig abwärtskompatibel mit dem 802.11b-Standard sind. • **802.11b + g** - Sowohl 802.11g als auch 802.11b-WLAN-Station können den WLAN-Breitbandrouter nutzen. • **802.11b + g + n** - 802.11g-, 802.11b- und 802.11n (Entwurf)-WLAN Stationen können den WLAN-Breitbandrouter nutzen. • **802.11 g + n** - Sowohl 802.11.g- als auch 802.11n- (Entwurf) WLAN-Stationen können den WLAN-Breitbandrouter nutzen. • **802.11n** - Nur 802.11n- (Entwurf) WLAN-Stationen können den WLAN-Breitbandrouter nutzen.

Channel No.	Wählen Sie hier den Kanal aus, den Sie für Ihr Wireless LAN verwenden möchten. • Sollte es zu Störungen kommt (z. B. Verbindungsabbrüche und / oder langsame Datenübertragung) testen Sie mehrere Kanäle, um einen geeigneten Kanal zu finden. • Wenn Sie mehrere Access Points verwenden, sollten benachbarte Access Points unterschiedliche Kanäle nutzen, um Störungen zu vermeiden.
Broadcast SSID	Wenn aktiviert, überträgt der WLAN-Breitbandrouter seine SSID. Dadurch können PCs und andere WLAN-Stationen den Access Point finden und die korrekte SSID verwenden Die Standard-SSID ist **WBR-6000**. Wenn diese Funktion deaktiviert ist, müssen PC-Nutzer die SSID und andere Details der WLAN-Schnittstelle manuell eingeben, damit Sie eine Verbindung zum Access Point herstellen können.
Wireless Security	
Current Setting	Hier werden die aktuellen Einstellungen für die WLAN-Sicherheit angezeigt. Standardmäßig ist die Funktion deaktiviert.
Configure	Klicken Sie auf diese Schaltfläche, um auf den Unterbildschirm für WLAN-Sicherheit zuzugreifen und Einstellungen anzuzeigen oder zu ändern. Näheres hierzu erfahren Sie im folgenden Abschnitt.
MAC Filter	
MAC Filter	Es gibt drei Optionen: • Disabled - Hiermit können Sie die Funktion deaktivieren. • Allow - Nur die in der Station gelisteten Clients können eine Verbindung mit dem WLAN-Router herstellen. Um die Liste der Stationen zu bearbeiten, klicken Sie auf „Set Station“. • Deny - Einem gelisteten Client wird der Zugriff auf den Access Point verwehrt. Andere haben jedoch über den Access Point noch immer Zugriff auf das Internet oder LAN.
Set Stations	Klicken Sie auf diese Schaltfläche, um die Kontrollstationen der MAC-Adressen zu verwalten.

Draft 802.11n Setting	
Bandwidth	Wählen Sie die gewünschte Bandbreite aus der Dropdown-Liste aus. 20MHz Only – Ein-Kanal-Bandbreite 40MHz Only – Zwei-Kanal-Bandbreite; Kanäle können kombiniert werden, um die Leistung zu verbessern. 20MHz/40MHz Auto – automatische Auswahl. Dies ist die Standardeinstellung. Der WLAN-Breitbandrouter wählt je nach Bedarf die passende Bandbreite aus. Beachten Sie, dass bei 20Mhz Only oder 40 MHz Only Verbindungsprobleme auftreten können, da die Einstellungen möglicherweise nicht den Client-Geräten entsprechen. Die automatische Auswahl wird nachhaltig empfohlen.
Protected Mode	Hier können Sie den geschützten Modus ein- oder ausschalten. Wenn der geschützte Modus aktiv ist, wird die Übertragung von 802.11n (Entwurf) als erste Priorität gehandhabt.

6.6. WLAN-Sicherheit

Klicken Sie auf die Schaltfläche „Configure“ in der Bildschirmanzeige *Wireless*. Es stehen drei Sicherheitsoptionen zur Auswahl:

- **Disabled** - Datenverschlüsselung ist deaktiviert.
- **WEP** - Daten werden unter Verwendung des WEP-Standards verschlüsselt.
- **WPA-PSK** - Daten werden unter Verwendung des WPA-PSK-Standards verschlüsselt. WPA-PSK ist ein neuerer Standard, der weitaus sicherer ist als WEP. Wenn alle WLAN-Stationen WPA-PSK unterstützen, sollten sie WPA-PSK anstelle von WEP verwenden.
- **WPA2-PSK** - Hierbei handelt es sich um eine Weiterentwicklung von WPA-PSK. Durch die Verwendung von AES (Advanced Encryption Standard) als Verschlüsselungsmethode ist die Sicherheit noch größer.
- **WPA-PSK and WPA2-PSK** - Mit dieser Methode (auch als „Mixed Mode“ bekannt) können Clients entweder WPA-PSK (mit TKIP) oder WPA2-PSK (mit AES) verwenden.

6.6.1. WEP WLAN-Sicherheit

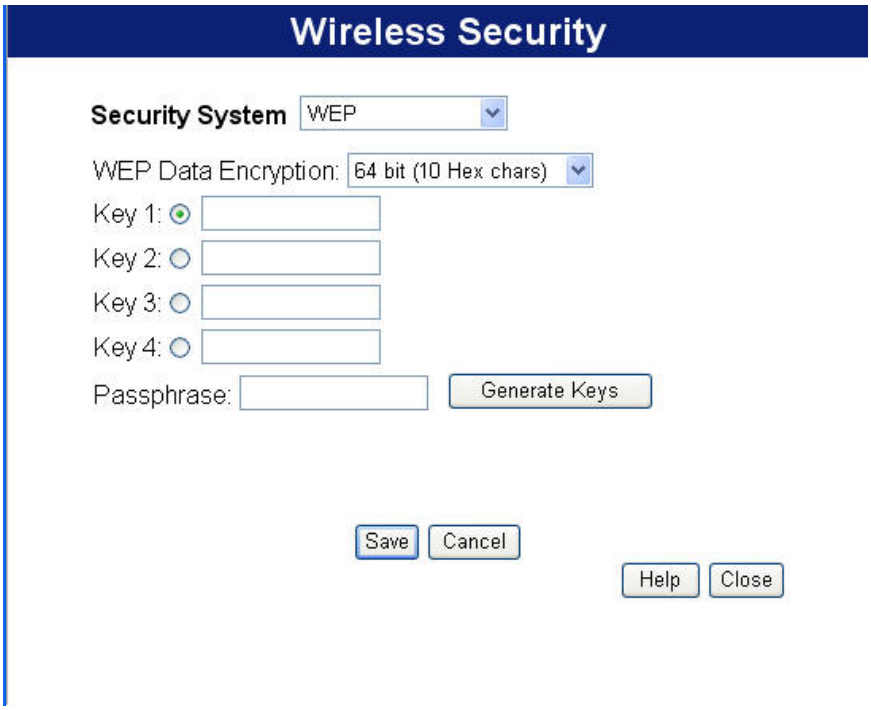


Abb. 9 WEP

Daten - Bildschirmanzeige WEP

WEP Data Encryption	
WEP Data Encryption	Wählen Sie die gewünschte Option, um die anderen WLAN-Stationen anzupassen. • **64 Bit** - Daten werden vor der Übertragung mithilfe des Standardschlüssels verschlüsselt. Hier ist mindestens die Eingabe des Standardschlüssels erforderlich. Bei einer 64-Bit-Verschlüsselung beträgt die Schlüssellänge 10 HEX-Zeichen (0-9 und A-F). • **128 Bit** - Daten werden vor der Übertragung mithilfe des Standardschlüssels verschlüsselt. Hier ist mindestens die Eingabe des Standardschlüssels erforderlich. Bei einer 128-Bit-Verschlüsselung beträgt die Schlüssellänge 26 HEX-Zeichen (0-9 und A-F).
Key 1 ~ 4	Wählen Sie hier einen Schlüssel als Standardschlüssel aus. Daten werden vor der Übertragung IMMER unter Verwendung dieses Standardschlüssels verschlüsselt. Die übrigen Schlüssel dienen ausschließlich zur Datenentschlüsselung. Für den **Standardschlüssel** ist die Eingabe eines **Schlüsselwerts** erforderlich.
Key Value	Geben Sie den / die gewünschten Schlüsselwert(e) ein. Die Eingabe des **Standardschlüssels** ist hierbei obligatorisch, die der anderen Schlüssel nur optional. Die übrigen WLAN-Stationen müssen den gleichen Schlüssen verwenden.
Passphrase	Anstatt den Schlüssel direkt einzugeben, können Sie auch einen Schlüssel erstellen, der auf einem Satz basiert. Geben Sie dazu den gewünschten Satz ein und klicken Sie auf die „Generate“-Schaltfläche.

6.6.2. WPA-PSK WLAN-Sicherheit

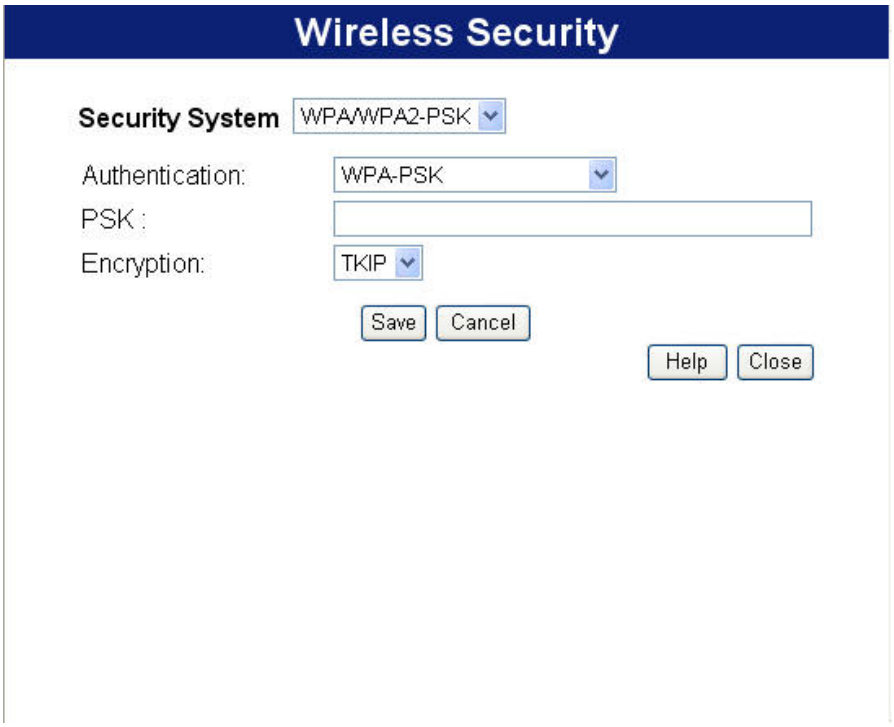


Abb. 10 WPA-PSK

Daten - Bildschirmanzeige WPA-PSK

Authentication	**WPA-PSK** Wie bei der WEP-Verschlüsselung werden die Daten vor der Übertragung verschlüsselt. WPA ist sicherer als WEP und sollte daher bevorzugt verwendet werden. WPA-PSK ist eine WPA-Version, die KEINEN Radiusserver im LAN erfordert.
PSK	Geben Sie einen PSK (Netzwerkschlüssel) ein. Die Datenverschlüsselung erfolgt unter Verwendung eines Schlüssels, der von diesem Netzwerkschlüssel abgeleitet wird. Die übrigen WLAN-Stationen müssen den gleichen Netzwerkschlüssel verwenden. Der Schlüsselwert muss eine Länge von 8 - 63 Zeichen haben.
WPA Encryption	Der WPA-PSK-Standard ermöglicht die Verwendung von verschiedenen Verschlüsselungsmethoden. Wählen Sie die gewünschte Option aus (TKIP oder AES). Die anderen WLAN-Stationen müssen dieselbe Verschlüsselungsmethode verwenden.

6.6.3. WPA2-PSK WLAN-Sicherheit

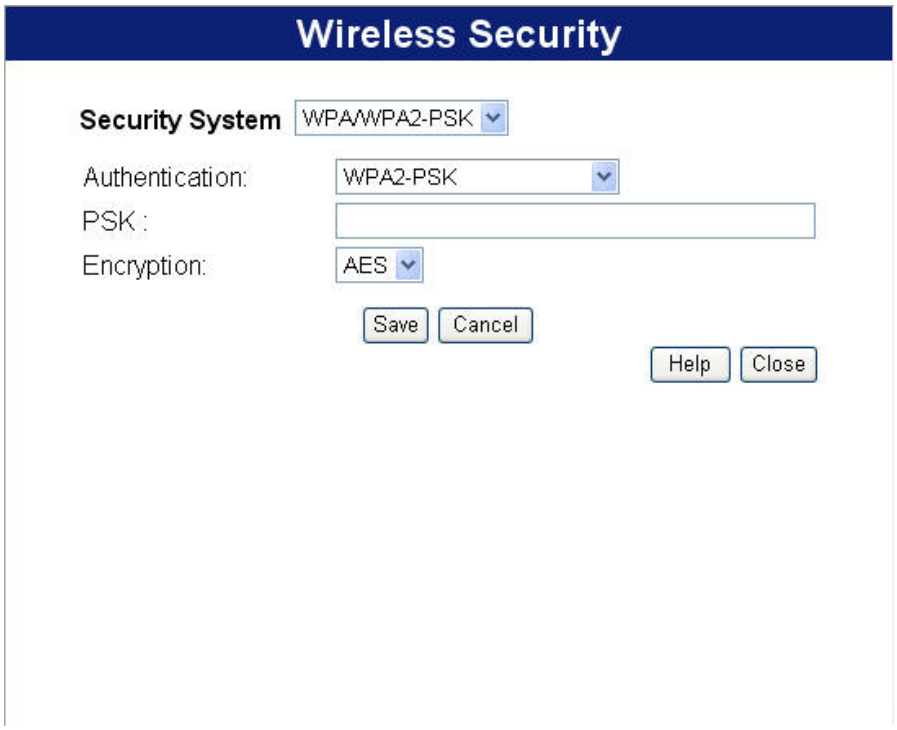


Abb. 11 WPA2-PSK

Daten - Bildschirmanzeige WPA2-PSK

Authentication	**WPA2-PSK** Hierbei handelt es sich um eine Weiterentwicklung von WPA-PSK. Durch die Verwendung von AES (Advanced Encryption Standard) als Verschlüsselungsmethode ist die Sicherheit noch größer.
PSK	Geben Sie einen PSK (Netzwerkschlüssel) ein. Die Datenverschlüsselung erfolgt unter Verwendung eines Schlüssels, der von diesem Netzwerkschlüssel abgeleitet wird. Die übrigen WLAN-Stationen müssen den gleichen Netzwerkschlüssel verwenden. Der Schlüsselwert muss eine Länge von 8 - 63 Zeichen haben.
Encryption	Bei WPA2-PSK ist als Verschlüsselungsmethode nur AES möglich. Beachten Sie, dass WLAN-Stationen dieselbe Verschlüsselungsmethode verwenden müssen.

6.6.4. WPA-PSK+WPA2-PSK WLAN-Sicherheit

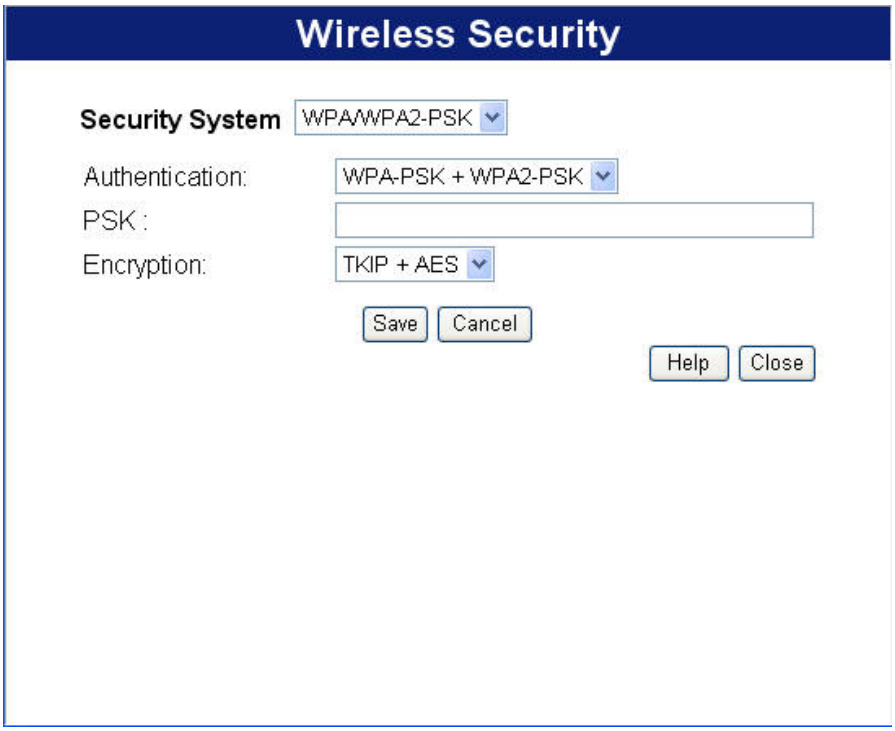


Abb. 12 WPA-PSK+WPA2-PSK

Daten - Bildschirmanzeige WPA-PSK+WPA2-PSK

Authentication	**WPA-PSK+WPA2-PSK** Mit dieser Methode (auch als „Mixed Mode“ bekannt) können Clients entweder WPA-PSK (mit TKIP) oder WPA2-PSK (mit AES) verwenden.
PSK	Geben Sie einen PSK (Netzwerkschlüssel) ein. Die Datenverschlüsselung erfolgt unter Verwendung eines Schlüssels, der von diesem Netzwerkschlüssel abgeleitet wird. Die übrigen WLAN-Stationen müssen den gleichen Netzwerkschlüssel verwenden. Der Schlüsselwert muss eine Länge von 8 - 63 Zeichen haben.
Encryption	Mit dem WPA/WPA2-PSK-Standard können verschiedene Verschlüsselungsmethoden zur gleichen Zeit verwendet werden. Die übrigen WLAN-Stationen müssen die gleiche Verschlüsselungsmethode verwenden.

6.7. Bildschirmanzeige Passwort

In der Bildschirmanzeige Passwort können Sie dem WLAN-Breitbandrouter ein Passwort zuweisen.

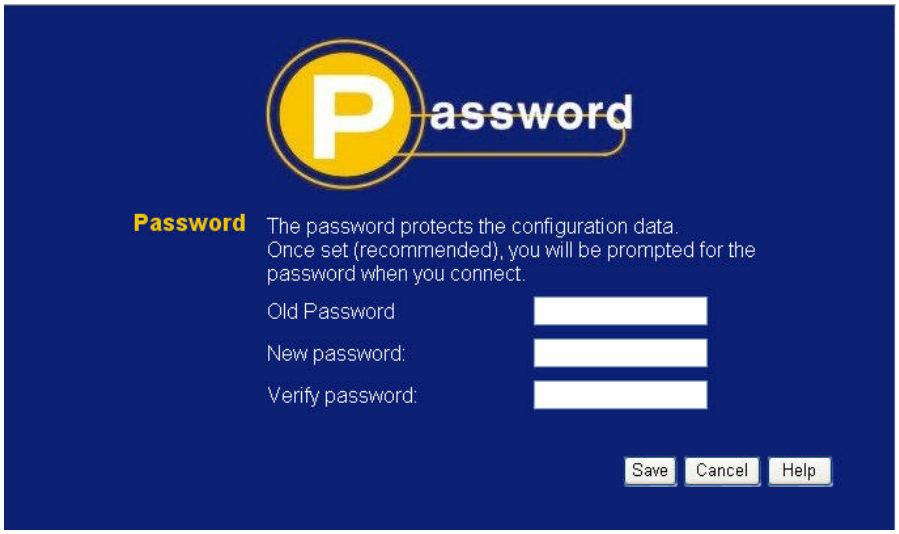


Abb. 13 Bildschirmanzeige Passwort

Old Password	Geben Sie hier das aktuelle Passwort ein.
New password	Geben Sie hier Ihr neues Passwort ein.
Verify password	Geben Sie hier zur Bestätigung Ihr neues Passwort erneut ein.

Beim Aufbau einer Verbindung werden Sie zur Eingabe des Passworts aufgefordert (siehe nachfolgendes Dialogfenster).

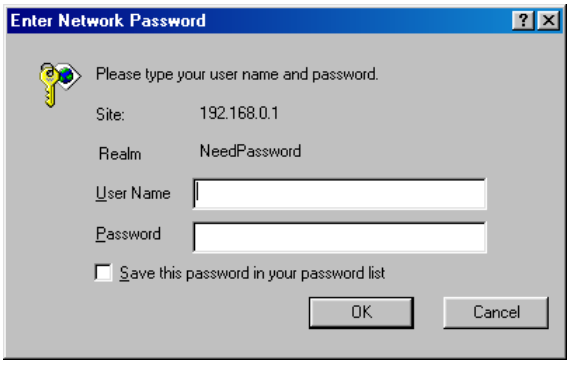


Abb. 14: Passwort-Dialogfenster

- Der Benutzername lautet immer „admin“.
- Geben Sie das Passwort für den WLAN-Breitbandrouter ein, wie in der Bildschirmanzeige *Passwort* oben angegeben. Das werkseitig voreingestellte Passwort ist **password**.

7. PC-Konfiguration

Diese Kapitel beschreibt die für das lokale („interne“) LAN erforderliche PC-Konfiguration.

7.1. Übersicht

Möglicherweise müssen an jedem PC folgende Konfigurationen vorgenommen werden:

- TCP/IP-Netzwerkeinstellungen
- Konfiguration des Internetzugangs
- WLAN-Konfiguration

7.2. Windows-Clients

Dieser Abschnitt beschreibt, wie Windows-Clients für den Internetzugang über den WLAN-Breitbandrouter konfiguriert werden.

Dazu müssen zunächst die TCP/IP-Einstellungen des PCs überprüft werden.

Der WLAN-Breitbandrouter nutzt das TCP/IP-Netzwerkprotokoll für alle Funktionen, weshalb es unabdingbar ist, dass das TCP/IP-Protokoll auf jedem PC installiert und konfiguriert ist.

7.2.1. TCP/IP-Einstellungen - Übersicht

Wenn Sie sowohl die Vorgabeeinstellungen des WLAN-Breitbandrouters als auch die Vorgabeeinstellungen von Windows für das TCP/IP-Protokoll verwenden, müssen keine Änderungen durchfgeführt werden.

- Der WLAN-Breitbandrouter dient in diesem Fall standardmäßig als DHCP-Server und weist jedem PC beim Hochfahren automatisch eine geeignete IP-Adresse (und die zugehörigen Informationen) zu.
- Für alle Nicht-Server-Versionen von Windows dient die TCP/IP-Standardeinstellung als DHCP-Client.

Wenn eine feste (spezifizierte) IP-Adresse benutzt wird, müssen die folgenden Änderungen durchgeführt werden:

- Der *Gateway* muss auf die IP-Adresse des WLAN-Breitbandrouters eingestellt werden.
- Der *DNS* muss auf die vom Internet-Service-Provider zugewiesene Adresse eingestellt werden.

Wenn Ihr LAN über einen Router verfügt, muss der LAN-Administrator den Router selbst konfigurieren. Weitere Informationen finden Sie in Kapitel 11 - Erweiterte Verwaltung.

7.2.2. Überprüfen der TCP/IP-Einstellungen - Windows 9x/ME

1. Klicken Sie auf *Systemsteuerung - Netzwerkeinstellungen*. Sie sollten nun folgende Bildschirmanzeige sehen:

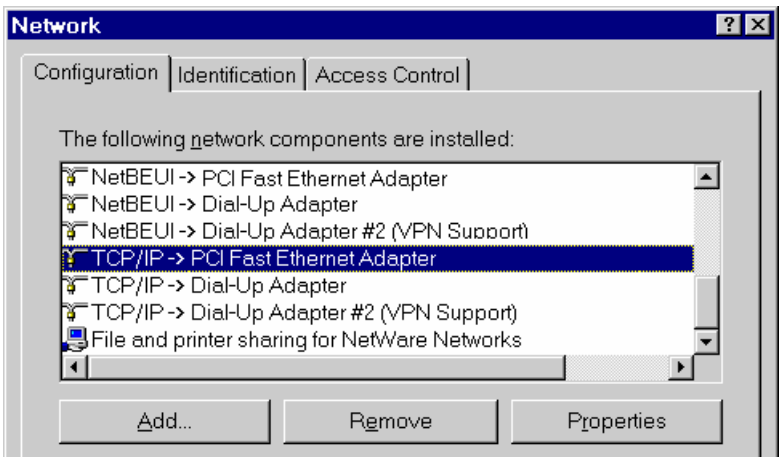


Abb. 15 Netzwerkkonfiguration

2. Wählen Sie das *TCP/IP*-Protokoll für Ihre Netzwerkkarte aus.
3. Klicken Sie auf *Eigenschaften*. Sie sollten nun folgende Bildschirmanzeige sehen.

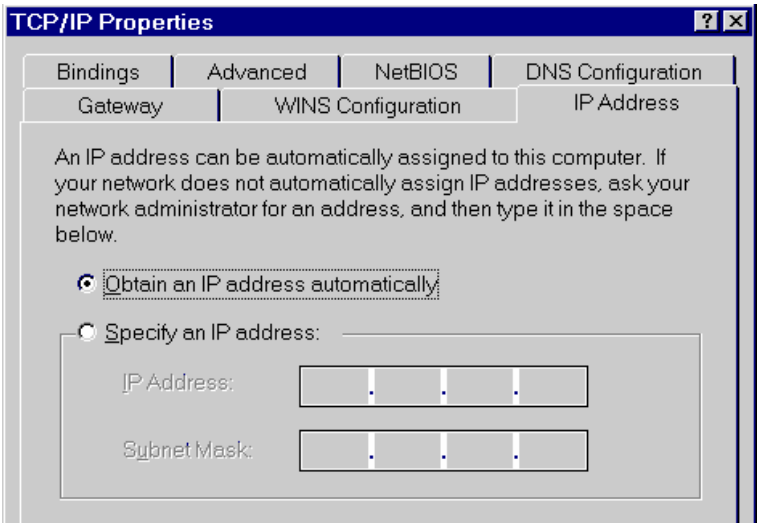

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

Abb. 16 IP-Adresse (Win 9x)

Gehen Sie folgendermaßen vor, um zu überprüfen, ob Ihre TCP/IP-Einstellungen korrekt sind:

Verwendung von DHCP

Um DHCP zu verwenden, aktivieren Sie *IP-Adresse automatisch beziehen*. Dies ist die Vorgabeeinstellung unter Windows. **Wir empfehlen die Verwendung dieser Einstellung**. Der WLAN-Breitbandrouter fungiert vorgabegemäß als DHCP-Server.

Starten Sie Ihren PC neu, um sicherzugehen, dass er eine IP-Adresse vom WLAN-Breitbandrouter erhält.

Verwendung von „Folgende IP-Adresse verwenden“

Wenn Ihr PC bereits konfiguriert ist, konsultieren Sie Ihren Netzwerkadministrator, bevor Sie die folgenden Änderungen durchführen:

- Geben Sie auf der Registerkarte *Gateway* die IP-Adresse des WLAN-Breitbandrouters im Feld *New Gateway* ein und klicken Sie auf *Add*, siehe Abbildung. Die IP-Adresse des WLAN-Breitbandrouters erhalten Sie von Ihrem LAN-Administrator.

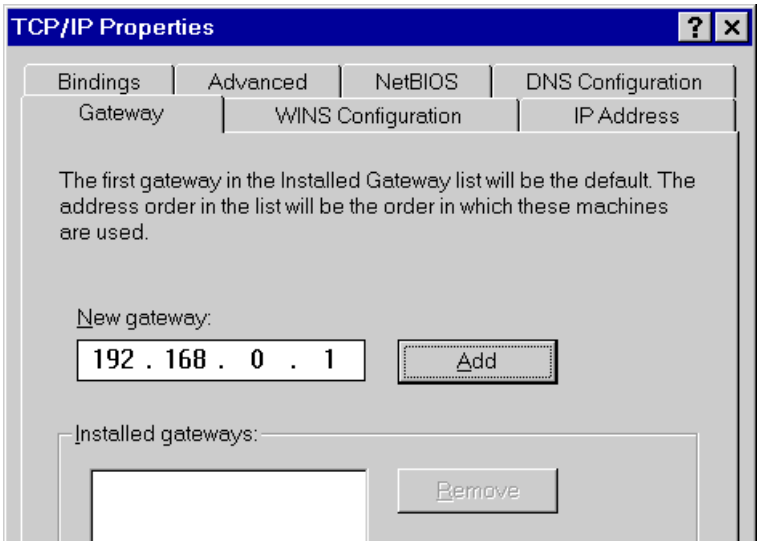


Abb. 17 Registerkarte Gateway (Win 9x)

- Überprüfen Sie auf der Registerkarte *DNS Configuration*, dass *Enable DNS* aktiviert ist. Wenn die *DNS Server Search Order*-Liste leer ist, geben Sie in den Feldern neben der Schaltfläche *Add* die DNS-Adresse ein, die von Ihrem ISP zur Verfügung gestellt wurde und klicken Sie dann auf *Add*.

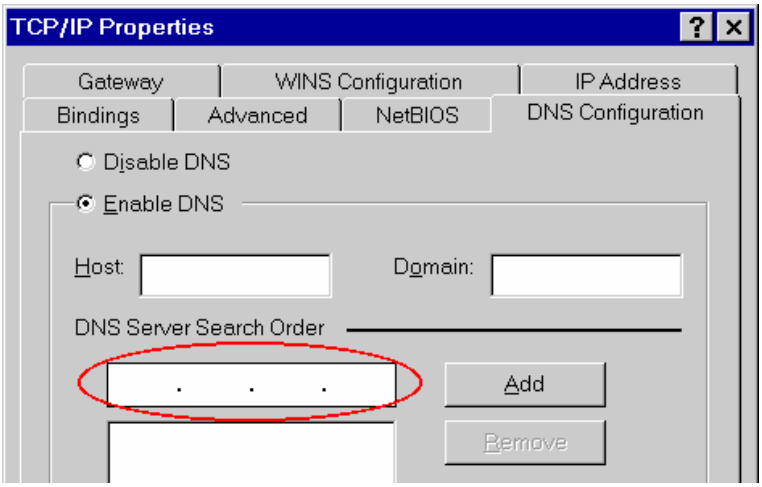


Abb. 18 Registerkarte DNS (Win 9x)

7.2.3. Überprüfen der TCP/IP-Einstellungen - Windows 2000

1. Klicken Sie auf *Systemsteuerung - Netzwerk- und DFÜ-Verbindung*.
2. Klicken Sie mit der rechten Maustaste auf das *LAN*-Symbol und wählen Sie *Eigenschaften*. Sie sollten nun folgende Bildschirmanzeige sehen:

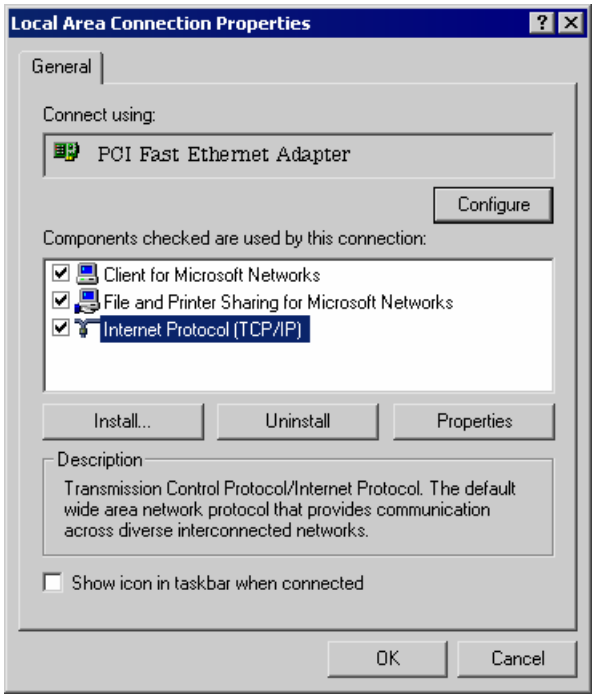


Abb. 19 Netzwerkkonfiguration (Win 2000)

3. Wählen Sie das *TCP/IP*-Protokoll für Ihre Netzwerkkarte aus.
4. Klicken Sie auf *Eigenschaften*. Sie sollten nun folgende Bildschirmanzeige sehen.

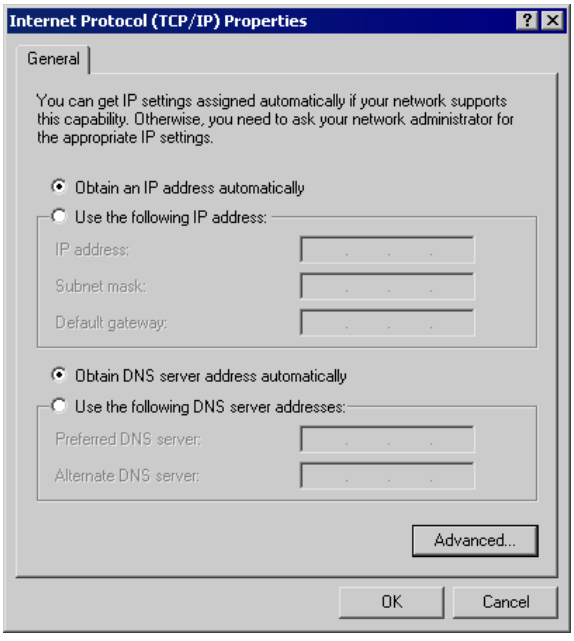

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Abb. 20 TCP/IP-Eigenschaften (Win 2000)

5. Gehen Sie folgendermaßen vor, um zu überprüfen, ob die TCP/IP-Einstellungen korrekt sind:

Verwendung von DHCP

Um DHCP zu verwenden, aktivieren Sie *IP-Adresse automatisch beziehen*. Dies ist die Vorgabeeinstellung unter Windows. **Wir empfehlen die Verwendung dieser Einstellung**. Der WLAN-Breitbandrouter fungiert vorgabegemäß als DHCP-Server.

Starten Sie Ihren PC neu, um sicherzugehen, dass er eine IP-Adresse vom WLAN-Breitbandrouter erhält.

Verwendung einer festen IP-Adresse („Folgende IP-Adresse verwenden“)

Wenn Ihr PC bereits konfiguriert ist, konsultieren Sie Ihren Netzwerkadministrator, bevor Sie die folgenden Änderungen durchführen.

- Geben Sie die IP-Adresse des WLAN-Breitbandrouters im *Default gateway*-Feld ein und klicken Sie auf *OK*. (Die IP-Adresse des WLAN-Breitbandrouters erhalten Sie von Ihrem LAN-Administrator.)
- Falls sich in den Feldern *DNS Server* keine Einträge befinden, klicken Sie auf *Folgende DNS-Serveradressen verwenden* und geben Sie die von Ihrem Internet-Service-Provider mitgeteilte(n) Adresse(n) ein. Klicken Sie anschließend auf *OK*.

7.2.4. Überprüfen der TCP/IP-Einstellungen - Windows XP

1. Klicken Sie auf *Systemsteuerung - Netzwerkverbindungen*.
2. Klicken Sie mit der rechten Maustaste auf das Symbol *LAN-Verbindung* und wählen Sie *Eigenschaften*. Sie sollten nun folgende Bildschirmanzeige sehen:

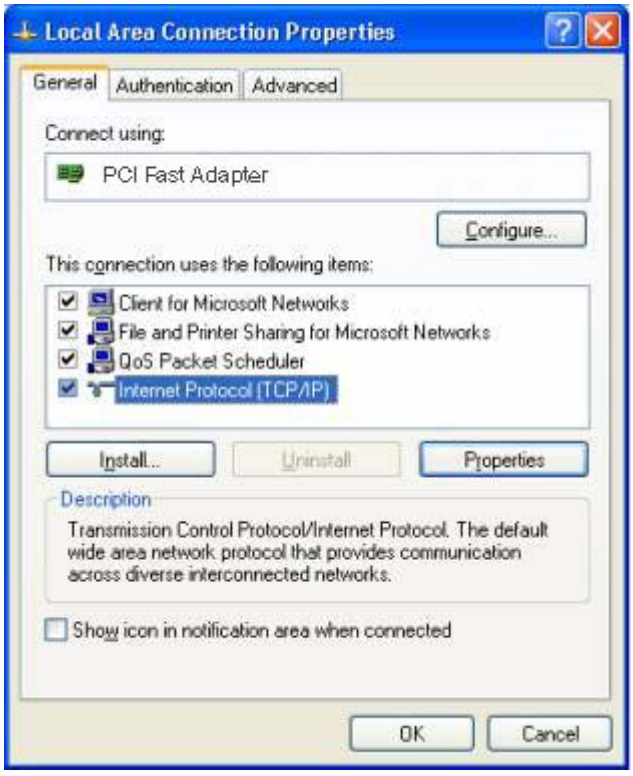


Abb. 21 Netzwerkkonfiguration (Windows XP)

3. Wählen Sie das *TCP/IP*-Protokoll für Ihre Netzwerkkarte aus.
4. Klicken Sie auf *Eigenschaften*. Sie sollten nun folgende Bildschirmanzeige sehen.

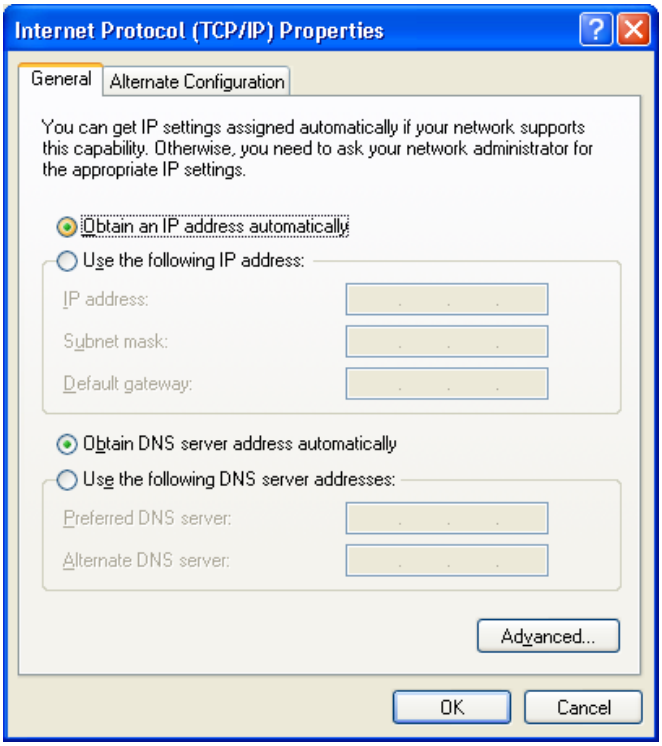

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Abb. 22 TCP/IP-Eigenschaften (Windows XP)

5. Gehen Sie folgendermaßen vor, um zu überprüfen, ob Ihre TCP/IP-Einstellungen korrekt sind.

Verwendung von DHCP

Um DHCP zu verwenden, aktivieren Sie *IP-Adresse automatisch beziehen*. Dies ist die Vorgabeeinstellung unter Windows. **Wir empfehlen die Verwendung dieser Einstellung**. Der WLAN-Breitbandrouter fungiert vorgabegemäß als DHCP-Server.

Starten Sie Ihren PC neu, um sicherzugehen, dass er eine IP-Adresse vom WLAN-Breitbandrouter erhält.

Verwendung einer festen IP-Adresse („Folgende IP-Adresse verwenden“)

Wenn Ihr PC bereits konfiguriert ist, konsultieren Sie Ihren Netzwerkadministrator, bevor Sie die folgenden Änderungen durchführen.

- Geben Sie die IP-Adresse des WLAN-Breitbandrouters im Feld *Default gateway* ein und klicken Sie auf *OK*. Die IP-Adresse des WLAN-Breitbandrouters erhalten Sie von Ihrem LAN-Administrator.
- Falls sich in den Feldern *DNS Server* keine Einträge befinden, klicken Sie auf *Folgende DNS-Serveradressen verwenden* und geben Sie die von Ihrem Internet-Service-Provider mitgeteilte(n) Adresse(n) ein. Klicken Sie anschließend auf *OK*.

7.2.5. Internetzugang

Um Ihre PCs so zu konfigurieren, dass sie den WLAN-Breitbandrouter für den Internetzugang benutzen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass DSL-Modem, Kabelmodem, oder eine andere permanente Verbindung funktionstüchig sind.
- Um Ihren Browser so zu konfigurieren, dass LAN für den Internetzugang verwendet wird anstatt einer DFÜ-Verbindung, gehen Sie wie folgt vor.

Bei Windows 9x/ME/2000

1. Gehen Sie auf *Start - Einstellungen - Systemsteuerung - Internetoptionen*.
2. Wählen Sie die Registerkarte Verbindungen und klicken Sie auf *Setup*.
3. Wählen Sie „Verbindung manuell einrichten“ oder „Verbindung über LAN (Local Area Network) einrichten“ und klicken Sie auf *Weiter*.
4. Wählen Sie „Verbindung über LAN (Local Area Network) einrichten“ und klicken Sie auf *Weiter*.
5. Stellen Sie sicher, dass alle Auswahlfelder in der folgenden Bildschirmanzeige zur Konfiguration der Internetverbindung über LAN **deaktiviert sind**.
6. Klicken Sie auf „Nein“, wenn die Meldung „Möchten Sie jetzt ein Internet-E-Mail-Account einrichten?“ eingeblendet wird.
7. Klicken Sie auf *Fertigstellen*, um den Assistenten für die Internetverbindung zu schließen.
   Die Einrichtung ist damit abgeschlossen.

Bei Windows XP

1. Gehen Sie auf *Start - Systemsteuerung – Netzwerk- und Internetverbindungen*.
2. Wählen Sie *Eigene Internetverbindung einrichten bzw. ändern*.
3. Wählen Sie die Registerkarte *Verbindungen* und klicken Sie auf *Setup*.
4. Schließen Sie das Pop-up-Fenster „Standortinformationen”.
5. Klicken Sie in der Bildschirmanzeige „Assistent für neue Verbindungen“ auf *Weiter*.
6. Wählen Sie „Verbindung mit dem Internet herstellen“ und klicken Sie auf *Weiter*.
7. Wählen Sie „Verbindung manuell einrichten“ und klicken Sie auf *Weiter*.
8. Wählen Sie „Verbindung über eine beständige aktive Breitbandverbindung herstellen“ und klicken Sie auf *Weiter*.
9. Klicken Sie auf *Fertigstellen*, um den Assistenten für neue Verbindungen zu schließen.
   Die Konfiguration ist damit abgeschlossen.

Zugang zu AOL

Um über den WLAN-Breitbandrouter auf AOL (America On Line) zuzugreifen, muss die *AOL für Windows*-Software so konfiguriert werden, dass sie einen TCP/IP-Netzwerkzugang anstatt einer DFÜ-Verbindung nutzt. Die folgenden Schritte müssen durchgeführt werden:

- Starten Sie die *AOL für Windows*-Kommunikationssoftware. Stellen Sie sicher, dass es sich um Version 2.5, 3.0 oder eine spätere handelt. Die Konfiguration ist mit früheren Versionen nicht möglich.
- Klicken Sie auf*Setup*.
- Wählen Sie *Standort hinzufügen* und ändern Sie den Standortnamen von „Neuer Standort“ zu „Wireless Broadband Router“.
- Klicken Sie auf*Standort bearbeiten*. Wählen Sie *TCP/IP* für das Feld *Netzwerk*. (Lassen Sie das Feld *Phone Number* frei).
- Klicken Sie auf *Speichern* und dann auf *OK*.
  Die Konfiguration ist damit abgeschlossen.
- Bevor Sie auf „Sign On“ klicken, sollten Sie immer sichergehen, dass Sie den Standort „Wireless Broadband Router“ als Speicherort benutzen.

7.3. Macintosh-Clients

Sie können von Ihrem Macintosh über den WLAN-Breitbandrouter auf das Internet zugreifen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie „Kontrollfelder“ und dann „TCP/IP“.
2. Wählen Sie aus dem Pop-up-Menü *Verbinden über* die Option *Ethernet*.
3. Wählen Sie aus dem Pop-up-Menü *Konfigurieren* die Option *Über DHCP-Server*. Das Feld „DHCP Client ID“ kann leer gelassen werden.
4. Schließen Sie das TCP/IP-Fenster und speichern Sie so Ihre Einstellungen.

Wenn Sie eine manuell zugeordnete IP-Adresse anstelle eines DHCP benutzen, lauten die notwendigen Änderungen wie folgt:

- Geben Sie in das Feld *Routeradresse* die IP-Adresse des WLAN-Breitbandrouters ein.
- Stellen Sie sicher, dass Ihre DNS-Einstellungen korrekt sind.

7.4. Linux-Clients

Um über den WLAN-Breitbandrouter Zugriff auf das Internet zu haben, ist es lediglich notwendig, den WLAN-Breitbandrouter als „Gateway“ einzustellen.

Stellen Sie sicher, dass Sie als „root“ eingeloggt sind, bevor Sie versuchen, Änderungen vorzunehmen.

Feste IP-Adresse

Die meisten UNIX-Umgebungen verwenden eine feste IP-Adresse. Wollen Sie weiterhin eine feste IP-Adresse verwenden, führen Sie folgenden Änderungen in Ihrer Konfiguration durch.

- Stellen Sie als Standard-Gateway die IP-Adresse des WLAN-Breitbandrouters ein.
- Stellen Sie sicher, dass Ihre DNS (Name Server)-Einstellungen korrekt sind.

Verwendung als DHCP-Client (empfohlen)

Die folgende Vorgehensweise kann je nach verwendeter Linux- und X-Windows Shell-Version variieren.

1. Starten Sie Ihren X-Windows-Clientcomputer.
2. Gehen Sie auf *Systemsteuerung - Netzwerk*.
3. Wählen sie für Ihre Netzwerkkarte den Eintrag „Schnittstelle“. Normalerweise ist hier die Schnittstelle „eth0“ eingetragen.
4. Klicken Sie auf *Bearbeiten*, stellen Sie unter „Protokoll“ „DHCP“ ein und speichern Sie ihre Änderungen.

5. Änderungen aktivieren:

- Verwenden Sie die Schaltflächen „Deaktivieren“ und „Aktivieren“, sofern diese vorhanden sind.
- ODER: Führen Sie einen Systemneustart durch.

7.5. Andere Unix-Systeme

Gehen Sie folgendermaßen vor, um über den WLAN-Breitbandrouter auf das Internet zuzugreifen:

- Stellen Sie sicher, dass im „Gateway“-Feld für Ihre Netzwerkkarte die IP-Adresse des WLAN-Breitbandrouters eingestellt ist.
- Stellen Sie sicher, dass Ihre DNS (Name Server)-Einstellungen korrekt sind.

7.6. Konfiguration der WLAN-Stationen

Diese Kapitel beschreibt, wie der Access Point des WLAN-Routers unabhängig von dem auf dem Client-computer installierten Betriebssystem verwendet werden kann.

Um die Funktion Wireless Access Point des WLAN-Breitbandrouters zu verwenden, müssen auf den WLAN-Stationen die entsprechenden Einstellungen vorgenommen werden:

Modus	Als Modus muss der Eintrag ***Infrastructure*** (anstelle von Ad-Hoc) eingestellt werden. Access Points funktionieren nur im ***Infrastruktur***-Modus.
SSID (ESSID)	Hier muss der gleiche Wert wie für den WLAN-Breitbandrouter verwendet werden. Die Standardeinstellung ist **WBR-6000**.
WLAN-Sicherheit	Standardmäßig ist beim WLAN-Breitbandrouter die WLAN-Sicherheitsfunktion nicht aktiviert. • Wenn die Sicherheit auf dem WLAN-Breitbandrouter de-aktiviert ist, muss sie auch an allen WLAN-Stationen deaktiviert werden. • Wenn die Sicherheit auf dem WLAN-Router aktiviert ist (WEP oder WPA-PSK), müssen bei allen Stationen die gleichen Einstellungen vorgenommen werden wie beim WLAN-Breitbandrouter.

8. Betrieb und Status

Dieses Kapitel erläutert den Betrieb des WLAN-Breitbandrouters und die Statusanzeigen.

8.1. Betrieb

Wenn sowohl der WLAN-Breitbandrouter als auch die PCs konfiguriert sind, erfolgt der weitere Betrieb automatisch.

In bestimmten Situationen kann jedoch zusätzliche Internetkonfiguration erforderlich sein. Näheres darüber erfahren Sie in *Kapitel 9 - Erweiterte Funktionen*.

8.2. Statusanzeige

Verwenden Sie den ***Status***-Link im Hauptmenü, um diesen Bildschirm zu öffnen.

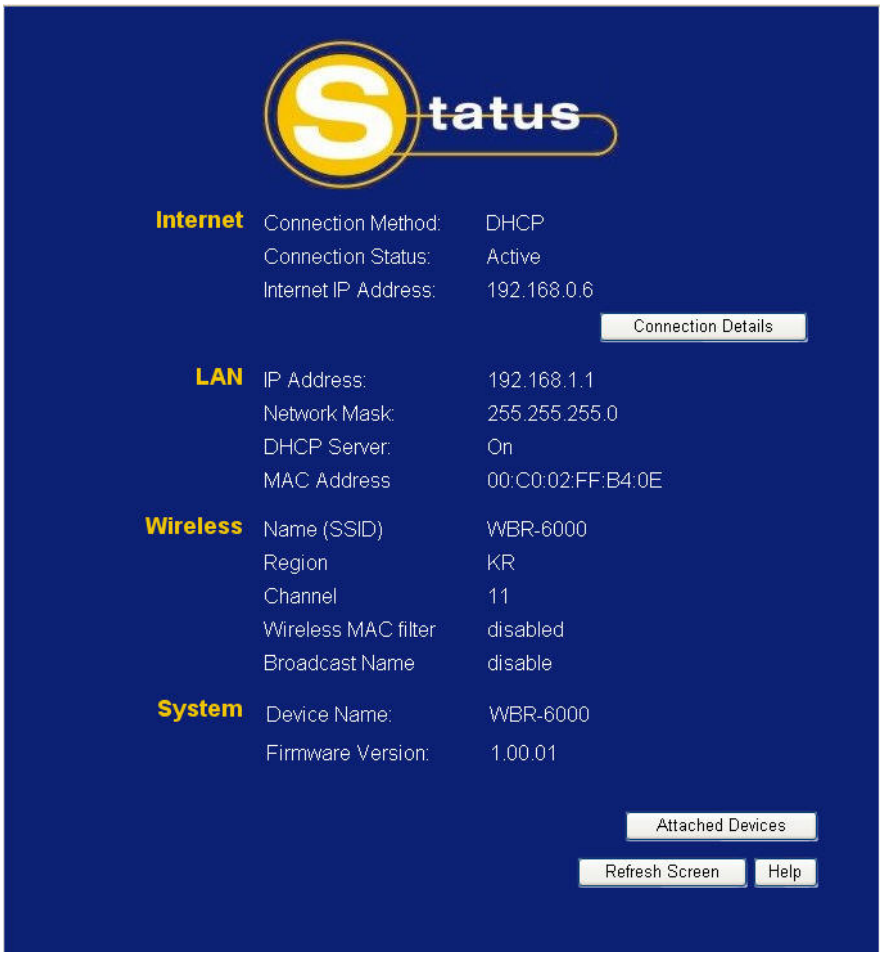


Abb. 23 Statusanzeige

Daten - Statusanzeige

Internet	
Connection Method	Zeigt das momentante Verbindungsverfahren an, das im *Einrichtungsassistenten* eingestellt wurde.

Connection Status	Hier wird der aktuelle Status der Internetverbindung angezeigt. • **Active** - Verbindung besteht. • **Idle** - Es besteht keine Verbindung, allerdings konnte auch kein Fehler gefunden werden. Dieser Zustand tritt normalerweise auf, wenn eine Leerlaufverbindung automatisch beendet wurde. • **Failed** - Die Verbindung wurde abweichend von der normalen Prozedur beendet, z. B. durch einen Modemausfall oder durch den Abbruch der Verbindung zum ISP-Server. Falls ein Fehler vorliegt, können Sie für weitere Informationen auf „Verbindungsdetails“ klicken.
Internet IP Address	Diese IP-Adresse wird vom ISP (Internet-Service-Provider) vergeben. Wenn Sie eine dynamische IP-Adresse verwenden und gegenwärtig keine Verbindung zum Internet besteht, ist dieser Eintrag leer.
Connection Details	Klicken Sie auf diese Schaltfläche, um ein Unterfenster zu öffnen und detaillierte Informationen zur aktuellen Verbindung zu erhalten. Je nach Verbindungstyp kann auch ein Log zur Verfügung stehen.
LAN	
IP Address	IP-Adresse des WLAN-Breitbandrouters
Network Mask	Netzwerkmaske (Subnetzmaske) für o. a. IP-Adresse
DHCP Server	Hier wird der Status der DHCP-Serverfunktion angezeigt. Die Serverfunktion kann aktiviert oder deaktiviert sein.
MAC Address	Dies ist die MAC-Adresse des WLAN-Breitbandrouters, die in der LAN-Schnittstelle angezeigt wird.

Wireless	
Name (SSID)	Wenn Sie ein ESS (Extended Service Set – Erweiterungsgerät mit mehreren Access Points) verwenden, wird diese ID als SSID bzw. ESSID (Extended Service Set Identifier) bezeichnet.
Region	Die aktuelle Region, wie in der Bildschirmanzeige Wireless eingestellt.
Channel	Zeigt den momentan genutzten Kanal an, wie in der Bildschirmanzeige Wireless eingestellt.
Wireless AP	Zeigt an, ob die Funktion Wireless Access Point aktiviert ist.
Broadcast Name	Zeigt an, ob die SSID übertragen wird. Diese Einstellung befindet sich in der Bildschirmanzeige Wireless.
System	
Device Name	Der aktuelle Name des Routers
Firmware Version	Die Version der aktuell installierten Firmware
Schaltflächen	
Connection Details	Klicken Sie auf diese Schaltfläche, um ein Unterfenster zu öffnen und detaillierte Informationen zur aktuellen Verbindung zu erhalten.
Attached Devices	Durch Anklicken öffnet sich ein Unterfenster, in dem alle aktuellen LAN- und WLAN-Geräte angezeigt werden.
Refresh Screen	Aktualisieren der auf dem Bildschirm angezeigten Daten

8.3. Verbindungsstatus - PPPoE

Bei Verwendung von PPPoE (PPP over Ethernet) erscheint nach Anklicken der Schaltfläche „Connection Details“ eine Anzeige ähnlich der folgenden.

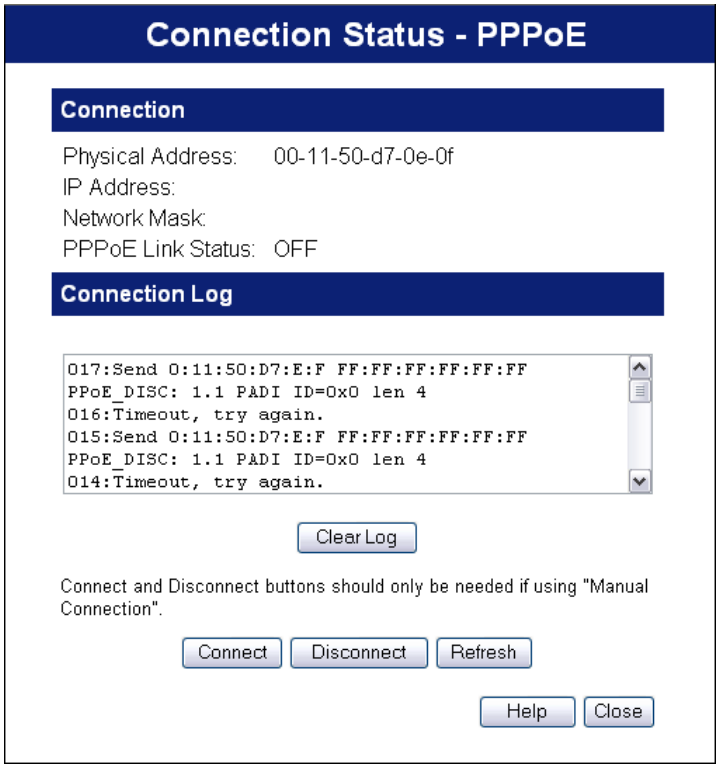


Abb. 24: PPPoE-Statusanzeige

Daten - Bildschirmanzeige PPPoE

Connection Time	Zeigt die Dauer der aktuellen Verbindung an.
Connection to Server	Zeigt an, ob eine Verbindung besteht.
Negotiation	Hier wird der Status des PPPoE Server-Logins angezeigt.
IP Address	Die IP-Adresse des Geräts, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Network Mask	Die Netzwerkmaske für die oben genannte IP-Adresse.

Schaltflächen	
Connect	Wenn keine Verbindung aktiv ist, stellen Sie über diese Schaltfläche eine Verbindung zu Ihrem ISP her.
Disconnect	Wenn Sie mit Ihrem ISP verbunden sind, können Sie die Verbindung über diese Schaltfläche beenden.
Close	Durch Klicken auf diese Schaltfläche wird das Fenster geschlossen.

8.4. Verbindungsstatus - PPTP

Wird PPTP (Peer-to-Peer Tunneling Protocol) verwendet, so wird beim Klicken auf die Schaltfläche „Connection Details“ ein Bildschirm wie der folgende angezeigt.

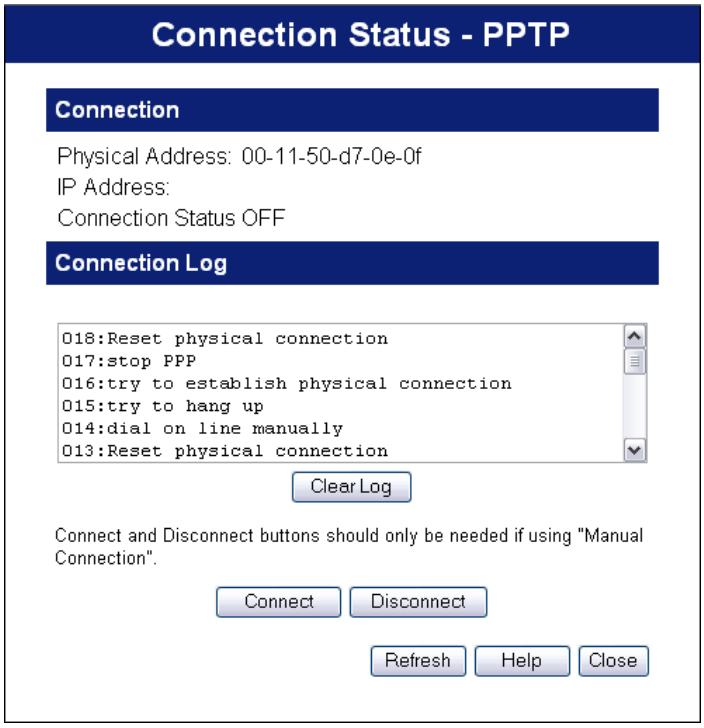


Abb. 25 PPTP-Statusanzeige

Daten - Bildschirmanzeige PPTP

Connection	
Physical Address	Die Hardwareadresse dieses Gerätes, wie sie von externen Geräten aus dem Internet gesehen wird. (Sie unterscheidet sich von der Hardwareadresse, die von Geräten im lokalen LAN gesehen wird).
IP Address	Die IP-Adresse des Geräts, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Connection Status	• Zeigt an, ob eine Verbindung besteht. • Falls die Verbindung nicht aktiv ist, klicken Sie auf *Connect*, um eine Verbindung herzustellen. • Wenn bereits eine Verbindung steht, klicken Sie auf *Disconnect* um die Verbindung zu beenden. • Normalerweise ist es nicht nötig, die Schaltflächen *Connect* und *Disconnect* zu verwenden, solange „Connect automatically, as required“ deaktiviert ist.

Connection Log	
Connection Log	• Das Verbindungslog zeigt Statusnachrichten bzgl. der bestehenden Verbindung an. • Die Schaltfläche „Clear Log“ startet das Log erneut, während die Schaltfläche „Refresh“ Meldungen auf dem Bildschirm aktualisiert.
Schaltflächen	
Connect	Wenn keine Verbindung aktiv ist, stellen Sie über diese Schaltfläche eine Verbindung zu Ihrem ISP her.
Disconnect	Wenn Sie mit Ihrem ISP verbunden sind, können Sie hier die Verbindung beenden.
Clear Log	Löscht alle Daten, die sich gegenwärtig im Log befinden. Dies vereinfacht es, neue Nachrichten zu lesen.
Refresh	Über diese Schaltfläche aktualisieren Sie die Daten auf dem Bildschirm.

8.5. Verbindungsstatus - L2TP

Wird L2TP genutzt, so wird beim Klicken auf die Schaltfläche „Connection Details“ ein Bildschirm wie der folgende angezeigt.

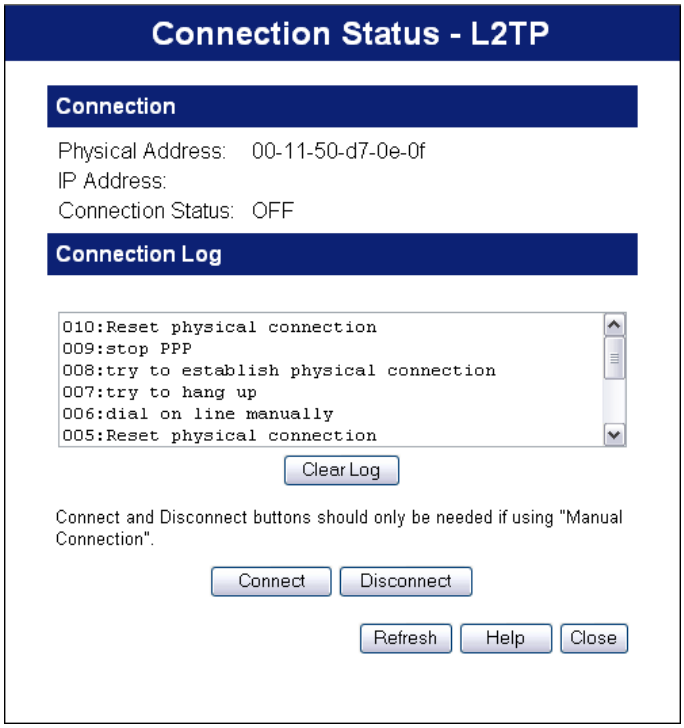


Abb. 26 L2TP-Statusanzeige

Daten - Bildschirmanzeige L2TP

Internet	
Physical Address	Die Hardwareadresse dieses Gerätes, wie sie von externen Geräten aus dem Internet gesehen wird. (Sie unterscheidet sich von der Hardwareadresse, die von Geräten im lokalen LAN gesehen wird).
IP Address	Die IP-Adresse des Geräts, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Connection Status	Zeigt an, ob eine Verbindung besteht. • Falls die Verbindung nicht aktiv ist, klicken Sie auf *Connect*, um eine Verbindung herzustellen. • Wenn bereits eine Verbindung steht, klicken Sie auf *Disconnect* um die Verbindung zu beenden. • Normalerweise ist es nicht nötig, die Schaltflächen *Connect* und *Disconnect* zu verwenden, solange „Connect automatically, as required“ deaktiviert ist.

Connection Log	
Connection Log	• Der Verbindungslog zeigt Statusnachrichten bzgl. der bestehenden Verbindung an. • Die Schaltfläche „Clear Log“ startet das Log erneut, während die Schaltfläche „Refresh“ Meldungen auf dem Bildschirm aktualisiert.
Schaltflächen	
Connect	Wenn keine Verbindung aktiv ist, stellen Sie über diese Schaltfläche eine Verbindung zu Ihrem ISP her.
Disconnect	Wenn Sie mit Ihrem ISP verbunden sind, unterbrechen Sie diese Verbindung über diese Schaltfläche.
Clear Log	Löscht alle Daten, die sich gegenwärtig im Log befinden. Dies vereinfacht es, neue Nachrichten zu lesen.
Refresh	Über diese Schaltfläche aktualisieren Sie die Daten auf dem Bildschirm.

8.6. Verbindungsstatus – Telstra Big Pond

Ein Beispielbildschirm ist unten abgebildet.

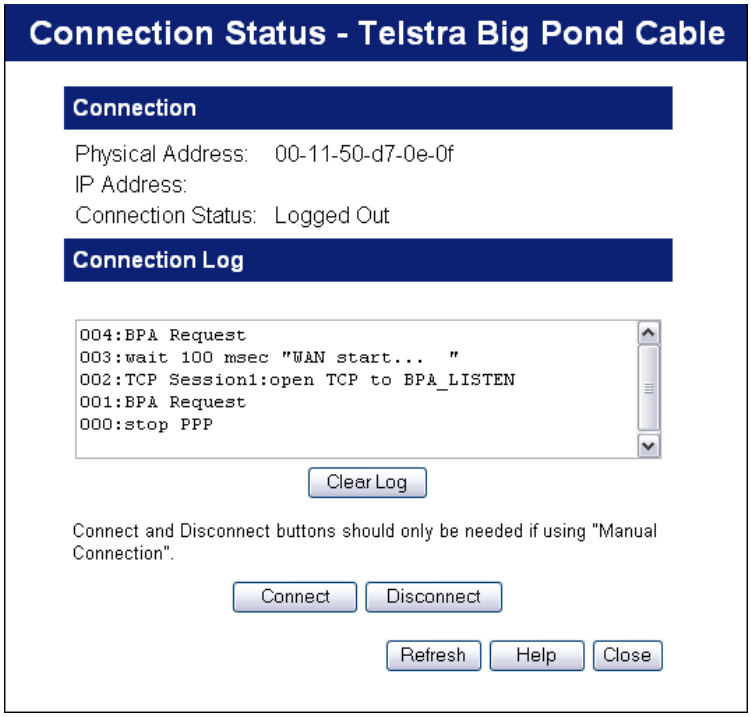


Abb. 27 Telstra Big Pond-Statusanzeige

Daten - Bildschirmanzeige Big Pond

Connection	
Physical Address	Die Hardwareadresse dieses Geräts, wie sie von externen Geräten gesehen wird (sie unterscheidet sich von der Hardwareadresse, die von Geräten im lokalen LAN gesehen wird).
IP Address	Die IP-Adresse des Geräts, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Connection Status	Zeigt an, ob eine Verbindung besteht. • Falls keine Verbindung besteht, klicken Sie auf „Connect“, um eine Verbindung herzustellen. • Wenn eine Verbindung besteht, klicken Sie auf „Disconnect“, um die Verbindung zu beenden. • Normalerweise ist es nicht nötig, die Schaltflächen „Connect“ und „Disconnect“ zu verwenden, solange „Connect automatically, as required“ deaktiviert ist.

Connection Log	
Connection Log	• Das Verbindungslog zeigt Statusmeldungen bezüglich der bestehenden Verbindung an. • Klicken Sie auf „Clear Log“, um das Log erneut zu starten und auf „Refresh“, um die Meldungen auf dem Bildschirm zu aktualisieren.
Schaltflächen	
Connect	Wenn keine Verbindung besteht, stellen Sie eine solche zu Telstra Big Pond her.
Disconnect	Wenn eine Verbindung zu Telstra Big Pond besteht, trennen Sie diese.
Clear Log	Löscht alle Daten, die sich gegenwärtig im Log befinden. Dies vereinfacht es, neue Nachrichten zu lesen.
Refresh	Über diese Schaltfläche aktualisieren Sie die Daten auf dem Bildschirm.

8.7. Verbindungsdetails - SingTel RAS

Wenn Sie die Zugriffsmethode SingTel RAS verwenden, wird beim Klicken auf die Schaltfläche „Connection Details“ ein Bildschirm wie der folgende angezeigt.

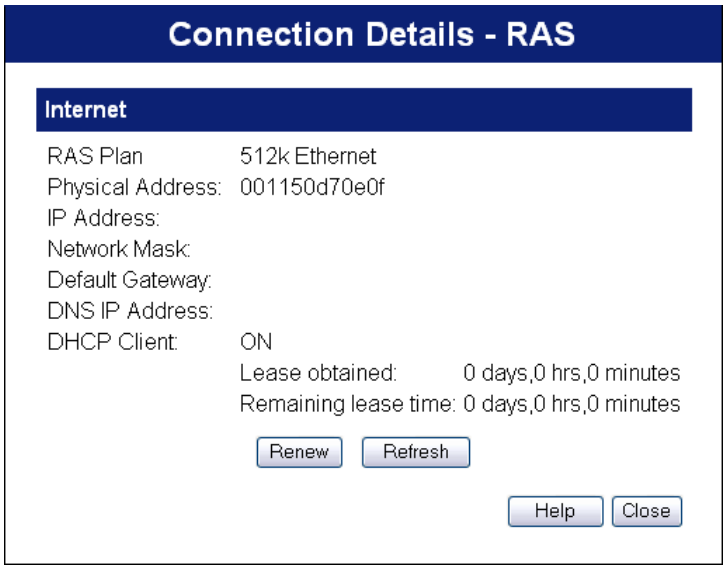


Abb. 28 Verbindungsdetails - RAS

Daten - Bildschirmanzeige RAS

Internet	
RAS-Plan	Der aktuell verwendete RAS-Plan (Verbindungsgeschwindigkeit)
Physical Address	Die Hardwareadresse dieses Geräts, wie sie von externen Geräten aus dem Internet gesehen wird. (Sie unterscheidet sich von der Hardwareadresse, die von Geräten im lokalen LAN gesehen wird).
IP Address	Die IP-Adresse des Geräts, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Network Mask	Die Netzwerkmaske für die oben genannte IP-Adresse.
Default Gateway	Die IP-Adresse des externen Gateways oder des Breitbandrouters, der mit der o. a. IP-Adresse verbunden ist.
DNS IP Address	Die IP-Adresse des Domain Name Servers, der gegenwärtig genutzt wird.
DHCP Client	• Sie können diese Funktion aktivieren oder deaktivieren. • Wenn die Funktion aktiviert ist, wird die Internet-IP-Adresse vom ISP automatisch bei der Verbindung vergeben (dynamische IP-Adresse). In diesem Fall

	müssen Sie die Details in die Felder „Lease obtained“ und „Remaining lease time“ eingeben. Das Nutzungsrecht wird bei Verfall automatisch erneuert. Benutzen Sie die Schaltfläche „Renew“, wenn Sie das Nutzungsrecht umgehend manuell erneuern wollen. • Wenn die Funktion deaktiviert ist, ist die IP-Adresse Ihres ISPs fest oder statisch. In diesem Fall kann die Schaltfläche „Release/Renew“ nicht verwendet werden.
Schaltflächen	
Release/Renew	Diese Schaltfläche wird nur dann verwendet, wenn die o. a. IP-Adresse bei der Verbindung automatisch vergeben wird (dynamische IP-Adresse). Andernfalls hat sie keine Funktion. • Auf der Schaltfläche steht „Release“, wenn der WLAN-Breitbandrouter eine IP-Adresse verwendet, die ihm vom DHCP-Server des ISPs zugewiesen wurde. Klicken Sie auf „Release“, um die IP-Adresse freizugeben und die Verbindung zu beenden. • Wenn „Renew“ auf der Schaltfläche steht, bedeutet das, dass die IP-Adresse für den WLAN-Breitbandrouter nicht vom DHCP-Server des ISPs stammt. Klicken Sie auf „Renew“, um die Verbindung wiederherzustellen und eine IP-Adresse vom DHCP-Server des ISP zu erhalten.
Refresh	Aktualisiert die auf dem Bildschirm angezeigten Daten.

8.8. Verbindungsdetails - Dynamische IP-Adresse

Wenn Ihre Verbindung „direkt“ (ohne Login) mit dynamischer IP-Adresse hergestellt wird, wird ein Bildschirm wie der folgende angezeigt, wenn Sie auf „Connection Details“ klicken.

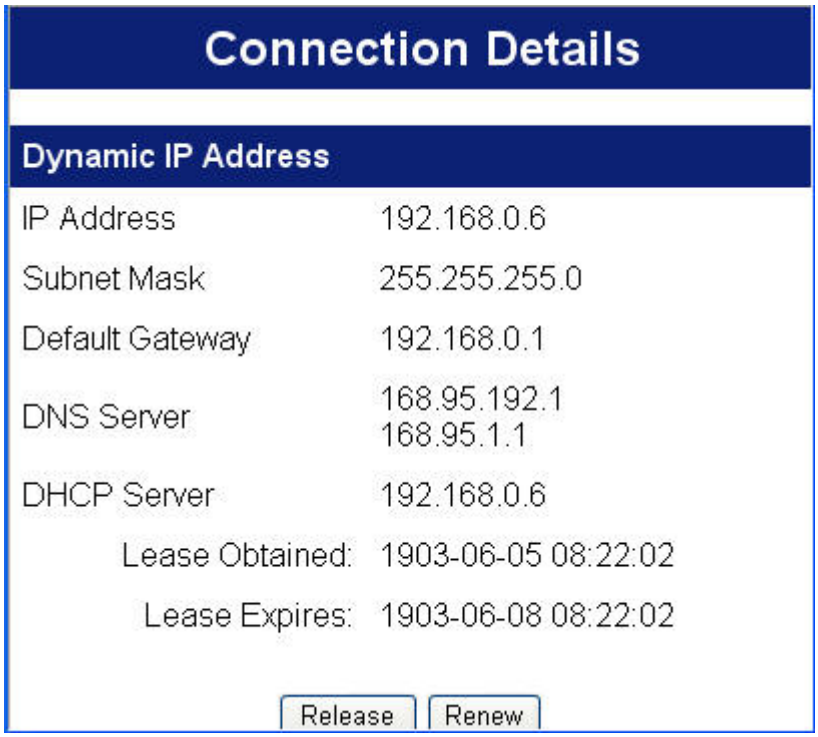


Abb. 29 Bildschirmanzeige Verbindungsdetails - Statische / dynamische IP-Adresse

Daten - Dynamische IP-Adresse

Internet	
IP Address	Die aktuelle IP-Adresse dieses Gerätes, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Subnet Mask	Die Subnetzmaske für die oben genannte IP-Adresse.
Default Gateway	Die IP-Adresse des externen Gateways oder des Routers, der mit der o.a. IP-Adresse verbunden ist.
DHCP Server	Die IP-Adresse des DHCP-Servers Ihres ISP.
DNS Server	Die IP-Adresse des Domain Name Servers, der gegenwärtig genutzt wird.
Lease Obtained **Lease Expires**	Hier wird angezeigt, wann die gegenwärtige IP-Adresse zugewiesen wurde und wie lange diese IP-Zuweisung (DHCP Lease) noch gültig ist.

Schaltflächen	
Release	Wenn dem WLAN-Breitbandrouter vom DHCP-Server des ISP eine IP-Adresse zugeordnet wurde, wird durch Klicken auf „Release“ die Verbindung unterbrochen und die IP-Adresse freigegeben.
Renew	Wenn der DHCP-Server des ISP dem WLAN-Breitbandrouter keine IP-Adresse zugewiesen hat, wird durch Klicken auf „Renew“ die Verbindung wiederhergestellt, um eine IP-Adresse vom DHCP-Server des ISP zu erhalten.
Close	Durch Klicken auf diese Schaltfläche wird das Fenster geschlossen.

8.9. Verbindungsdetails - Statische IP-Adresse

Wenn Ihre Verbindung „direkt“ (ohne Login) mit einer festen IP-Adresse hergestellt wird, wird ein Bildschirm wie der folgende angezeigt, wenn Sie auf „Connection Details“ klicken.

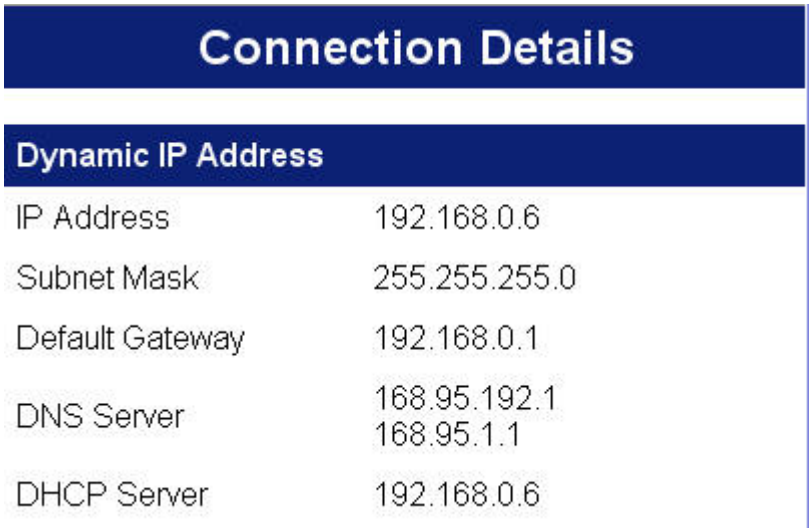


Abb. 30 Bildschirmanzeige Verbindungsdetails - Statische / dynamische IP-Adresse

Daten – Feste IP-Adresse

Internet	
IP Address	Die IP-Adresse des Geräts, wie sie von Internetnutzern gesehen wird. Diese Adresse wird durch Ihren ISP zugewiesen.
Subnet Mask	Die Subnetzmaske für die oben genannte IP-Adresse.
Default Gateway	Die IP-Adresse des externen Gateways oder des Routers, der mit der o.a. IP-Adresse verbunden ist.
DNS Server	Die IP-Adresse des Domain Name Servers, der gegenwärtig genutzt wird.

9. Erweiterte Funktionen

Dieses Kapitel beschreibt die „erweiterten“ Leistungsmerkmale des WLAN-Breitbandrouters und deren Funktionen.

9.1. Übersicht

Die folgenden erweiterten Funktionen stehen zur Verfügung:

- Internet:
- DMZ
- URL-Filter
- Zugriffskontrolle
- Dynamischer DNS
- Firewall-Regeln
- Firewall-Dienste
- Virtuelle Server
- Optionen
- Zeitpläne

9.2. Internet

Dieser Bildschirm ermöglicht den Zugriff auf die Funktionen DMZ und URL-Filter.

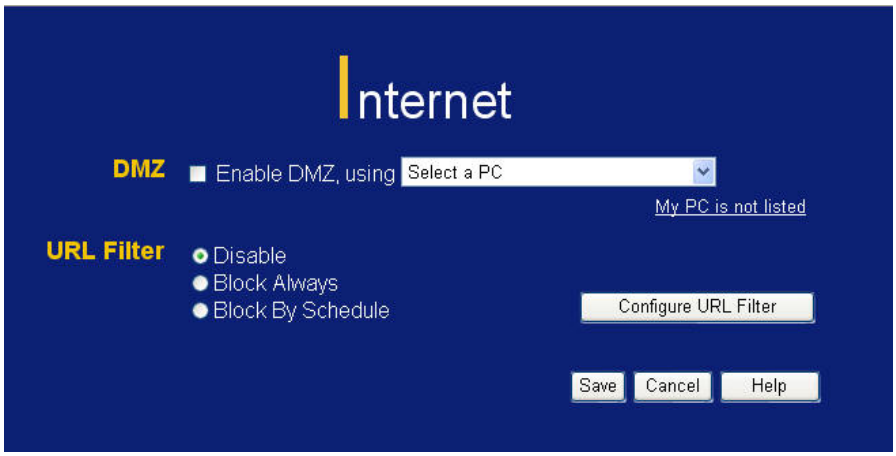


Abb. 31 Bildschirmanzeige Internet

9.2.1. DMZ

Wenn diese Funktion aktiviert ist, ist der DMZ-Computer Ihres LAN für alle Internetnutzer zugänglich.

- Dadurch kann praktisch jede Anwendung auf dem „DMZ-PC“ genutzt werden.
- Der „DMZ-PC“ empfängt alle „unbekannten“ Verbindungen und Daten.
- Bei aktivierter DMZ-Funktion müssen Sie den PC für die Nutzung als „DMZ-PC“ einstellen.

Der „DMZ-PC“ ist außerhalb der Firewall, was ihn anfälliger für Angriffe von außen macht. Aus diesem Grund sollten Sie die DMZ-Funktion nur aktivieren, wenn es notwendig ist.

9.2.2. URL-Filter

Mit dieser Funktion können Sie den Zugriff auf bestimmte Internetseiten einschränken. Der URL-Filter prüft jeden Zugriff auf eine Website. Der Zugriff wird verweigert, wenn die gesamte URL oder ein Teil davon mit den Einträgen in der Liste der zu sperrenden Internetseiten übereinstimmt.

Nehmen Sie die gewünschten Einstellungen in der Bildschirmanzeige *Advanced Internet* vor:

- **Disable** - Deaktiviert die Funktion.
- **Block Always** - Die Blockierung erfolgt ständig, unabhängig von den Einstellungen unter *Schedule*.
- **Block By Schedule** - Die Blockeriung erfolgt gemäß der Einstellungen unter *Schedule*.

Klicken Sie auf **Configure URL Filter**, um die Bildschirmanzeige URL-Filter zu öffnen. Dort können Sie Filtereinstellungen eingeben oder ändern, die festlegen, welche Seiten gesperrt werden.

Die Bildschirmanzeige ***URL-Filter*** wird angezeigt, wenn Sie auf **Configure URL Filter** in der Bildschirmanzeige *Advanced Internet* klicken.

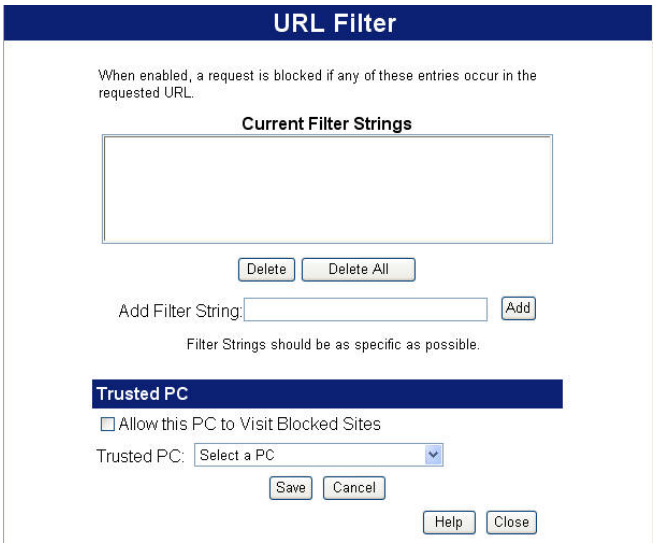


Abb. 32 Bildschirmanzeige URL-Filter

Daten - Bildschirmanzeige URL-Filter

Current Filter Strings	
Current Filter Strings	Diese Liste enthält alle blockierten Websites. • Klicken Sie auf „Add“, um weitere Websites hinzuzufügen. • Über **Delete** können Sie vorher markierte Einträge löschen. • Klicken Sie auf **Delete All**, um alle Einträge zu löschen.
Add Filter String	Um der aktuellen Liste einen Eintrag hinzuzufügen, geben Sie ein Wort oder einen Domainnamen ein und klicken Sie dann auf **Add**. Die Einträge sollten so präzise wie möglich sein, damit nicht mehr Websites blockiert werden als gewünscht.
Trusted PC	
Allow Trusted PC	Durch Aktivieren dieser Funktion ermöglichen Sie einem Computer uneingeschränkten Zugriff auf das Internet. Für den ausgewählten PC ist der URL-Filter deaktiviert. Wenn diese Funktion aktiviert ist, müssen Sie bestimmen, welcher PC der „privilegierte PC“ sein soll.
Trusted PC	Wählen Sie hier den „privilegierten PC“ aus.

9.3. Zugriffskontrolle

Über den Link *Access Control* im Menü Erweitert können Sie diese Funktion aufrufen.

9.3.1. Übersicht

Mit dieser Funktion können Administratoren die Zugriffsmöglichkeiten von PCs auf Ihrem LAN begrenzen. Mit den vorgegebenen Einstellungen hat jeder unbegrenzten Zugriff auf das Internet.

Die Einschränkungen entstehen durch das Blockieren von Diensten oder Verbindungsarten. Alle üblichen Dienste sind vordefiniert.
Wenn nötig, können Sie außerdem Ihre eigenen Dienste definieren.

9.3.2. Bildschirmanzeige Zugriffskontrolle

Um diesen Bildschirm aufzurufen, gehen Sie über den Link *Access Control* im Menü Erweitert.

Abb. 33 Bildschirmanzeige Zugriffskontrolle

Daten - Bildschirmanzeige Zugriffskontrolle

Internet Access	
Restrictions	Wählen Sie die gewünschten Optionen für die aktuelle Gruppe: • **None** - Nichts wird blockiert. Verwenden Sie diese Funktion, um die am wenigsten einschränkende Gruppe zu erstellen. • **Block all Internet access** - Der gesamte Verkehr über den WAN-Port wird blockiert. Verwenden Sie diese Funktion, um die am meisten einschränkende Gruppe zu erstellen. • **Block selected Services** - Hier können Sie auswählen, welche Dienste blockiert werden sollen. Verwenden Sie diese Funktion, um die Feinsteuerung über den Internetzugang für eine Gruppe zu erhalten.
Block by Schedule	Wenn der Internetzugang blockiert wird, können Sie festlegen, dass die Blockierung nur während vorher definierter Zeiten stattfindet. (Wenn der Zugang nicht blockiert wird, ist keine Zeitsteuerung möglich und diese Einstellung hat keine Wirkung.)
Trusted PCs	
Enable Trusted PCs	Markieren Sie die Checkbox, wenn Sie diese Funktion verwenden möchten.
Set Trusted PCs	Klicken Sie auf diese Schaltfläche, um der aktuellen Gruppe PCs hinzuzufügen oder sie aus der Gruppe zu entfernen. Nähere Details über *privilegierte PCs* finden Sie im nächsten Abschnitt.
Schaltflächen	
Save	Speichert die Daten auf dem Bildschirm.
Cancel	Macht alle Änderungen, die Sie seit dem letzten „Speichern“ durchgeführt haben, rückgängig.
Refresh	Über diese Schaltfläche aktualisieren Sie die Daten auf dem Bildschirm.

9.3.3. Bildschirmanzeige Privilegierte PCs

Klicken Sie auf *Set Trusted PCs* in der Bildschirmanzeige *Access Control*, um diesen Bildschirm zu öffnen.

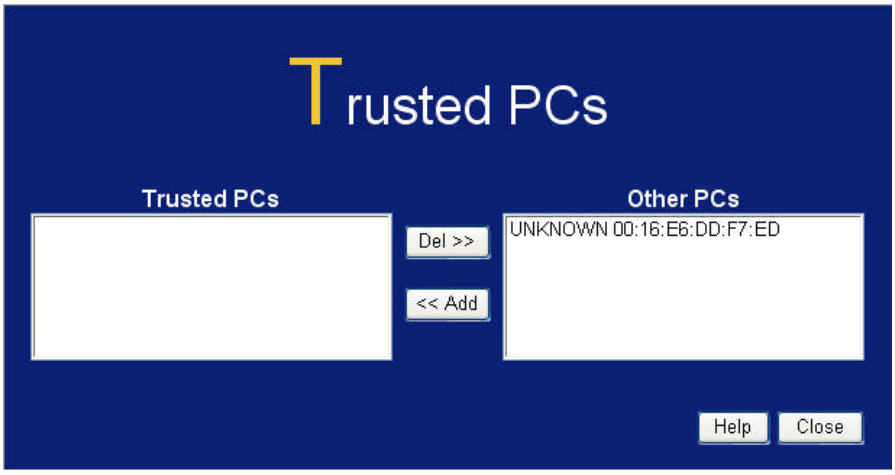


Abb. 34 Bildschirmanzeige Privilegierte PCs

In dieser Bildschirmanzeige können Sie der aktuellen Gruppe Mitglieder (PCs) hinzufügen oder sie aus der Gruppe entfernen.

- Markieren Sie einen PC und klicken Sie auf „Del >>“ (in der Liste der *privilegierten PCs*), um diesen aus der aktuellen Gruppe zu entfernen.
- Mit „<< Add“ können Sie der aktuellen Gruppe einen PC hinzufügen (aus der Liste der *anderen PCs*).

9.4. Dynamischer DNS (Domain Name Server)

Dieser kostenlose Dienst erweist sich als sehr nützlich in Verbindung mit der Funktion *Virtual Server*. So können Internetnutzer eine Verbindung mit Ihrem virtuellen Server über eine URL anstelle einer IP-Adresse herstellen.

Dadurch löst sich auch das Problem einer dynamischen IP-Adresse. Da diese sich mit jeder Verbindungsaufnahme ändert, kann sich die Verbindungsaufnahme als schwierig erweisen.

Der DDNS-Dienst funktioniert folgendermaßen:

1. Sie müssen sich zunächst bei einem der aufgelisteten Provider für DDNS-Dienste registrieren lassen.
2. Nach der Registrierung können Sie mithilfe des normalen Vorgangs des Dienstanbieters Ihren gewünschten Domainnamen anfordern.
3. Geben Sie Ihre DDNS-Daten auf dem DDNS-Bildschirm des WLAN-Breitbandrouters ein, um die DDNS-Funktion zu aktivieren.
4. Der WLAN-Breitbandrouter stellt dann automatisch sicher, dass Ihre aktuelle IP-Adresse im Domainnamenserver des DDNS-Dienstanbieters eingetragen wird.
5. Internetnutzer können sich dann mit Ihrem Domainnamen bei Ihren virtuellen Servern (oder DMZ-PCs) anmelden, wie in dieser Bildschirmanzeige deutlich wird.

9.4.1. Bildschirmanzeige DDNS

Wählen Sie *Advanced* im Hauptmenü und dann *Dynamic DNS*, um den nachfolgenden Bildschirm aufzurufen:

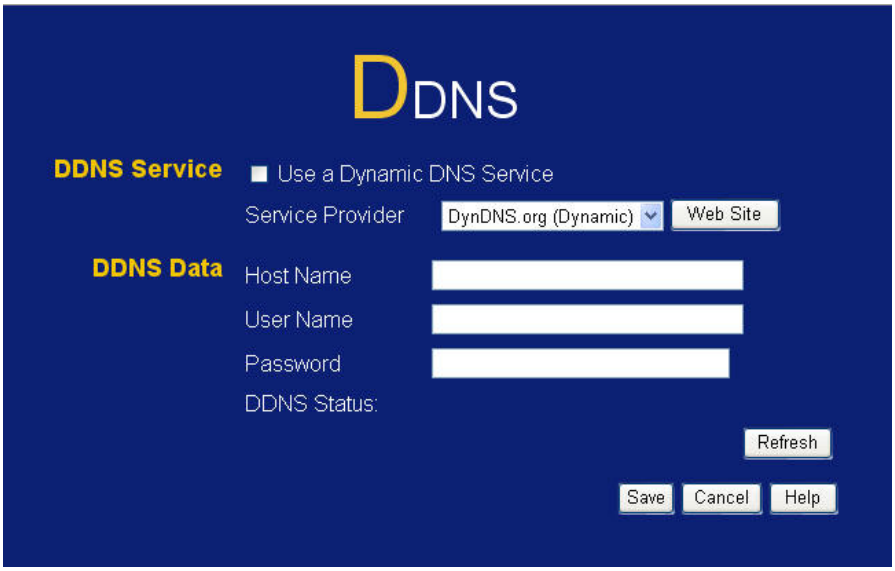


Abb. 35 Bildschirmanzeige DDNS

Daten - Bildschirmanzeige DDNS

DDNS Service	
Use a Dynamic DNS Service	Über dieses Kontrollkästchen können Sie die DDNS-Funktion nach Bedarf aktivieren und deaktivieren.
Service Provider	Wählen Sie hier den gewünschten DDNS-Provider.
Web Site	Klicken Sie auf diese Schaltfläche, um ein neues Fenster zu öffnen und eine Verbindung mit der Website des ausgewählten DDNS-Anbieters herzustellen.
DDNS Data	
Host Name	Geben Sie hier den Domainnamen ein, der Ihnen vom DDNS-Dienst zugewiesen wurde. Falls Sie mehr als einen Namen besitzen, geben Sie den Namen ein, den Sie verwenden möchten.
User Name	Geben Sie hier Ihren Benutzernamen für den DDNS-Dienst ein. (TZO.com verwendet Ihre E-Mail-Adresse.)
Password	Geben Sie hier Ihr aktuelles Passwort für den DDNS-Dienst an. (TZO.com nennt dies „Key“.)
DDNS Status	• Hierbei handelt es sich um eine vom DDNS-Server gesendete Meldung. • Sie lautet normalerweise „Update successful“. • Wenn die Meldung einen Fehler anzeigt, setzen Sie sich mit Ihrem DDNS-Dienstanbieter in Verbindung und beheben Sie das Problem.

9.5. Firewall-Regeln

Im Bildschirm ***Firewall Rules*** können Sie Regeln für die Firewall definieren, um bestimmten Datenverkehr zu erlauben oder zu blockieren. Mit Datenverkehr ist ein versuchter Verbindungsaufbau gemeint, nicht etwa die Übertragung von Datenpaketen.

Standardeinstellungen:

- Ausgehender Datenverkehr ist uneingeschränkt erlaubt.
- Eingehender Datenverkehr wird ausnahmslos abgewiesen.

Aufgrund dieser Voreinstellungen wird der **abgehende** Datenverkehr durch neue Regeln grundsätzlich **blockiert** und der **eingehende** Datenverkehr grundsätzlich **zugelassen**.

9.5.1. Bildschirmanzeige Firewall-Regeln

Ein Beispielbildschirm ist unten abgebildet.

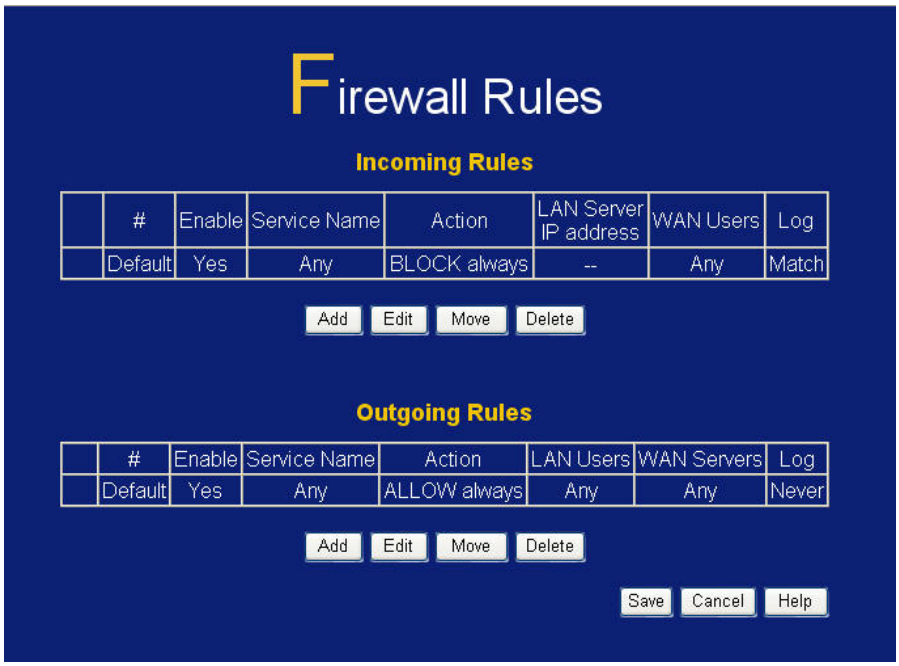

Firewall Rules
Incoming Rules
Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always -- Any Match
Add Edit Move Delete
Outgoing Rules
Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Save Cancel Help

Abb. 36 Bildschirmanzeige Firewall-Regeln

Daten - Bildschirmanzeige Firewall-Regeln

Incoming Rules	
#	Bei der Standardeinstellung erscheint hier „Default“. Wenn Sie selbst Regeln definieren, erscheint hier eine Optionsschaltfläche, über die Sie die Regel auswählen können.
Enable	Hier wird angezeigt, ob die Regel gegenwärtig aktiviert ist. Bei von Ihnen selbst definierten Regeln erscheint in dieser Spalte ein Kontrollkästchen, über das Sie die jeweilige Regel aktivieren oder deaktivieren können. (Um Änderungen zu speichern, klicken Sie auf „Save“.)
Service Name	Hier ist der Dienst aufgeführt, für den die Regel gilt.
Action	Die Aktion, die bei Verbindungen ausgeführt wird, auf die sich die Regel bezieht.
LAN Server IP Address	Hier ist der PC oder Server Ihres LAN aufgeführt, der als Empfänger von dieser Regel betroffen ist.
WAN Users	Die WAN-IP-Adresse, für die die jeweilige Regel gilt.
Log	Hier wird angezeigt, ob Verbindungen, für die diese Regel gilt, protokolliert werden.
Schaltflächen	Über die Schaltfläche *Add* können Sie eine neue Regel hinzufügen. Die übrigen Schaltflächen - *Edit*, *Move*, oder *Delete* - setzen voraus, dass Sie vorher eine Regel festgelegt haben. Die Auswahl einer Regel erfolgt über die Optionsschaltflächen in der linken Spalte.
Outgoing Rules	
#	Bei der Standardeinstellung erscheint hier „Default“. Wenn Sie selbst Regeln definieren, erscheint hier eine Optionsschaltfläche, über die Sie die Regel auswählen können.
Enable	Hier wird angezeigt, ob die Regel gegenwärtig aktiviert ist. Bei von Ihnen selbst definierten Regeln erscheint in dieser Spalte ein Kontrollkästchen, über das Sie die jeweilige Regel aktivieren oder deaktivieren können. (Um Änderungen zu speichern, klicken Sie auf „Save“.)
Service Name	Hier ist der Dienst aufgeführt, für den die Regel gilt.
Action	Die Aktion, die bei Verbindungen ausgeführt wird, auf die sich die Regel bezieht.

LAN Users	Hier sind einer oder mehrere LAN-PCs aufgeführt, für die die Regel gilt.
WAN Servers	WAN-IP-Adresse, für die die jeweilige Regel gilt
Log	Hier wird angezeigt, ob Verbindungen, für die diese Regel gilt, protokolliert werden.
Schaltflächen	Über die Schaltfläche *Add* können Sie eine neue Regel hinzufügen. Die übrigen Schaltflächen - *Edit*, *Move*, oder *Delete* - setzen voraus, dass Sie vorher eine Regel festgelegt haben. Die Auswahl einer Regel erfolgt über die Optionsschaltflächen in der linken Spalte.

9.5.2. Eingangsregeln (eingehende Dienste)

Dieser Bildschirm erscheint, wenn Sie unter „Incoming Rules“ auf die Schaltflächen „Add“ oder „Edit“ klicken.

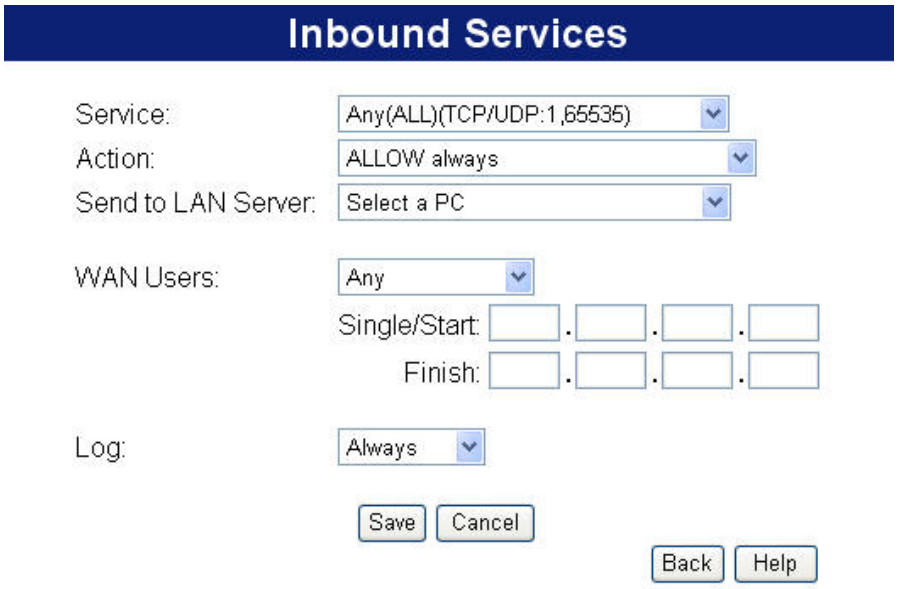


Abb. 37 Bildschirmanzeige Eingehende Dienste

Daten - Bildschirmanzeige Eingehende Dienste

Inbound Services	
Service	Wählen Sie hier den gewünschten Dienst aus. Hierdurch legen Sie fest, für welche Datenpakete die jeweilige Regel gilt. Wenn erforderlich, können Sie auf dem „Services“-Bildschirm einen neuen Dienst definieren, indem Sie die Protokolle und Portnummern des jeweiligen Dienstes angeben.

Action	Wählen Sie die gewünschte Aktion für Datenpakete, bei denen diese Regel angewendet wird: • ALLOW always (immer erlauben) • ALLOW by schedule, otherwise Block (temporär erlauben, sonst sperren) • BLOCK always (immer sperren) • BLOCK by schedule, otherwise Allow (temporär sperren, sonst erlauben) **Hinweis:** • Jeder Eingangsverkehr, der nicht durch von Ihnen definierte Regeln erlaubt wird, wird durch die Standardregel gesperrt. • BLOCK-Regeln sind nur dann von Nutzen, wenn für den jeweiligen Verkehr bereits eine ALLOW-Regel definiert wurde. (Sie dienen folglich dazu, bestimmten Verkehr zu sperren, der gegenwärtig aufgrund einer ALLOW-Regel durchgelassen wird.) • In der Bildschirmanzeige „Schedule" können Sie einen Zeitplan für Regeln definieren.
Send to LAN Server	Wählen Sie hier den PC oder Server Ihres LAN aus, der den von der jeweiligen Regel betroffenen eingehenden Verkehr empfangen soll.
WAN Users	Hier legen Sie durch die Eingabe der (WAN) IP-Adresse fest, für welche Datenpakete die jeweilige Regel gelten soll. Wählen Sie die gewünschte Option: • **Any** - Die jeweilige Regel gilt für alle IP-Adressen. • **Single address** - Bei dieser Option ist es erforderlich, dass Sie eine Adresse in das Feld „Single/Start“ eingeben. • **Address range** - Wenn Sie diese Funktion auswählen, ist es erforderlich, dass Sie Einträge in den Feldern „Single/Start“ und „Finish“ vornehmen, um den Adressbereich festzulegen.

Log	Hier legen Sie fest, ob Datenpakete, für die die jeweilige Regel gilt, protokolliert werden. Wählen Sie die gewünschte Aktion aus. • **Always** - Verkehr, auf den die Regel angewendet wird, wird immer protokolliert. (Dies ist nützlich, wenn Sie Ihre Regeln debuggen.) • **Never** - Verkehr, auf den die Regel angewendet wird, wird niemals protokolliert. • **Match** - Verkehr wird nur protokolliert, wenn er von der Regel betroffen ist. (Die Aktion wird durch die Regel bestimmt.) • **Not Match** - Verkehr, auf den die Regel angewendet wird, wird nur dann protokolliert, wenn er nicht von der Regel betroffen ist. (Die Aktion wird nicht durch die Regel bestimmt.)

9.5.3. Ausgangsregeln (ausgehende Dienste)

Dieser Bildschirm erscheint, wenn Sie unter „Outgoing Rules“ auf die Schaltflächen „Add“ oder „Edit“ klicken.

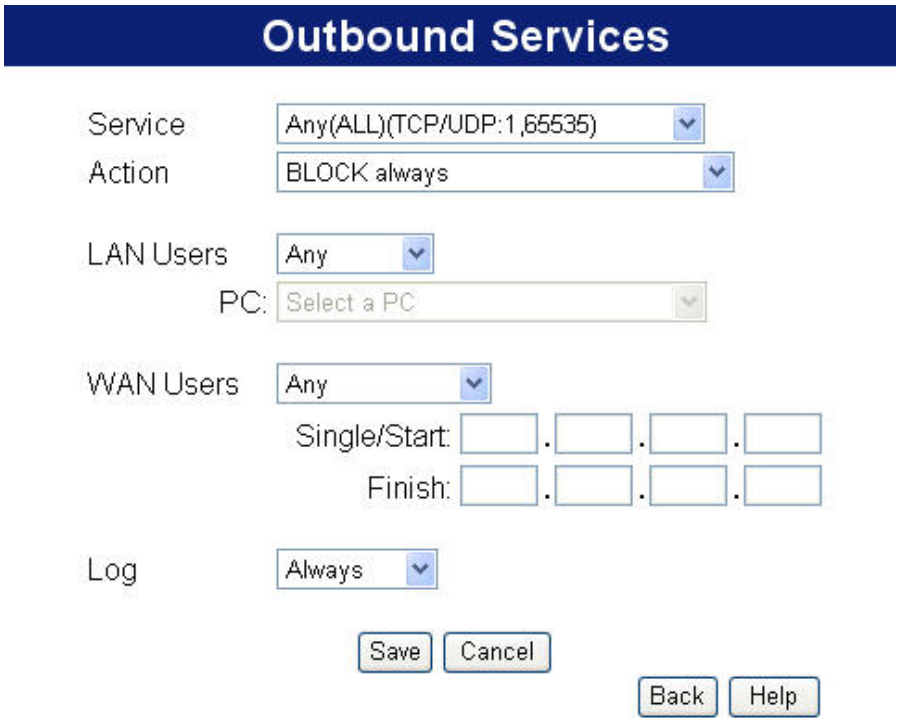


Abb. 38 Bildschirmanzeige Ausgehende Dienste

Daten - Bildschirmanzeige Ausgehende Dienste

Outbound Services	
Service	Wählen Sie hier den gewünschten Dienst oder die gewünschte Anwendung aus, für die diese Regel gelten soll. Wenn der gewünschte Dienst bzw. die gewünschte Anwendung nicht in der Liste erscheint, müssen Sie diese über die Bildschirmanzeige „Services“ festlegen.

Action	Wählen Sie die gewünschte Aktion für Datenpakete, bei denen diese Regel angewendet wird: • BLOCK always (immer sperren) • BLOCK by schedule, otherwise Allow (temporär sperren, sonst erlauben) • ALLOW always (immer erlauben) • ALLOW by schedule, otherwise Block (temporär erlauben, sonst sperren) **Hinweis:** • Ausgehender Verkehr, der nicht durch von Ihnen definierte Regeln gesperrt wird, wird durch die Standardregel erlaubt. • ALLOW-Regeln sind nur dann von Nutzen, wenn für den jeweiligen Verkehr bereits eine BLOCK-Regel definiert wurde. (Sie dienen folglich dazu, bestimmten Verkehr zu erlauben, der gegenwärtig aufgrund einer BLOCK-Regel gesperrt wird.) • In der Bildschirmanzeige „Schedule“ können Sie einen Zeitplan für Regeln definieren.
LAN Users	Wählen Sie hier aus, für welche PCs die Regel gelten soll. • **Any** - Die jeweilige Regel gilt für alle PCs. • **Single PC** - Die Regel gilt nur für einen PC. In diesem Fall muss der betreffende PC ausgewählt werden. **PC** - In der Einstellung Single PC müssen Sie den PC oder Server im LAN auswählen, auf den die Regel Bezug nimmt.
WAN Users	Hier legen Sie durch die Eingabe der (WAN) IP-Adresse fest, für welche Datenpakete die jeweilige Regel gelten soll. Wählen Sie die gewünschte Option: • **Any** - Die jeweilige Regel gilt für alle IP-Adressen. • **Single address** - Bei dieser Option ist es erforderlich, dass Sie eine Adresse in das Feld „Single/Start“ eingeben. • **Address range** - Wenn Sie diese Funktion auswählen, ist es erforderlich, dass Sie Einträge in den Feldern „Start“ und „Finish“ vornehmen.

Log	Hier legen Sie fest, ob Datenpakete, für die die jeweilige Regel gilt, protokolliert werden. Wählen Sie die gewünschte Aktion aus. • **Always** - Verkehr, auf den die Regel angewendet wird, wird immer protokolliert. (Dies ist nützlich, wenn Sie Ihre Regeln debuggen.) • **Never** - Verkehr, auf den die Regel angewendet wird, wird niemals protokolliert. • **Match** - Verkehr wird nur protokolliert, wenn er von der Regel betroffen ist. (Die Aktion wird durch die Regel bestimmt.) • **Not Match** - Verkehr, auf den die Regel angewendet wird, wird nur dann protokolliert, wenn er nicht von der Regel betroffen ist. (Die Aktion wird nicht durch die Regel bestimmt.)

9.6. Firewall-Dienste

Hier sehen Sie eine Liste der verfügbaren Dienste beim Anlegen von Firewall-Regeln.
Wenn Sie eine Firewall-Regel erstellen, der erforderliche Dienst jedoch nicht in der Liste ist, können Sie den erforderlichen Dienst mit dieser Funktion festlegen. Nach dem Anlegen befindet sich der Dienst dann in der Liste und kann beim Erstellen von Firewall-Regeln verwendet werden.

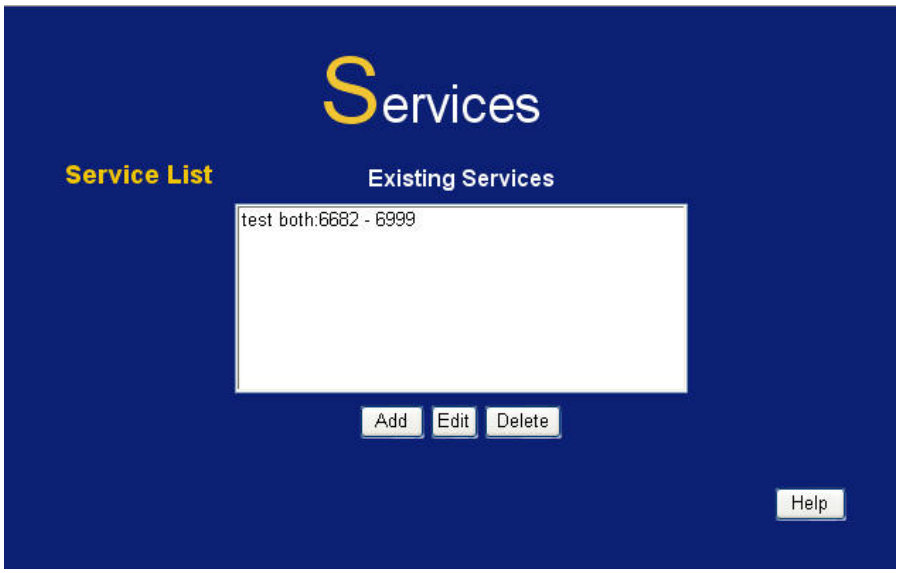


Abb. 39 Bildschirmanzeige Dienste

Daten - Bildschirmanzeige Dienste

Services	
Existing Services	Eine Liste aller definierten Dienste. Wenn Sie keine Dienste definiert haben, bleibt diese Liste leer. Wenn Sie Dienste definieren, tauchen Sie in dieser Liste auf, und werden außerdem in der Liste zum Erstellen von Firewall-Regeln angezeigt. (Benutzerdefinierte Dienste stehen am Ende der Liste nach den vordefinierten Diensten.)
Add	Durch Klicken auf diese Schaltfläche öffnet sich ein Unterfenster, in dem Sie neue Dienste hinzufügen können.
Edit	Durch Klicken auf diese Schaltfläche können Sie einen vorher ausgewählten Dienst bearbeiten.
Delete	Durch Klicken auf diese Schaltfläche können Sie vorher ausgewählte Dienste löschen. Sie können jeden beliebigen Dienst löschen, den Sie selbst definiert haben.

9.7. Virtuelle Server

Diese Funktion, die auch als *Port Forwarding* (Portweiterleitung) bekannt ist, ermöglicht es, Server im LAN für Internetnutzer zugänglich zu machen. Normalerweise können Internetnutzer auf einen Server in Ihrem LAN nicht zugreifen, wenn:

- der Server keine gültige, externe IP-Adresse hat.
- Versuche, die Geräte auf Ihrem LAN zu verbinden durch die Firewall dieses Geräts blockiert werden.

Die Funktion „Virtual Server“ löst diese Probleme und gestattet es Internetnutzern, sich mit Ihren Servern wie unten dargestellt zu verbinden.

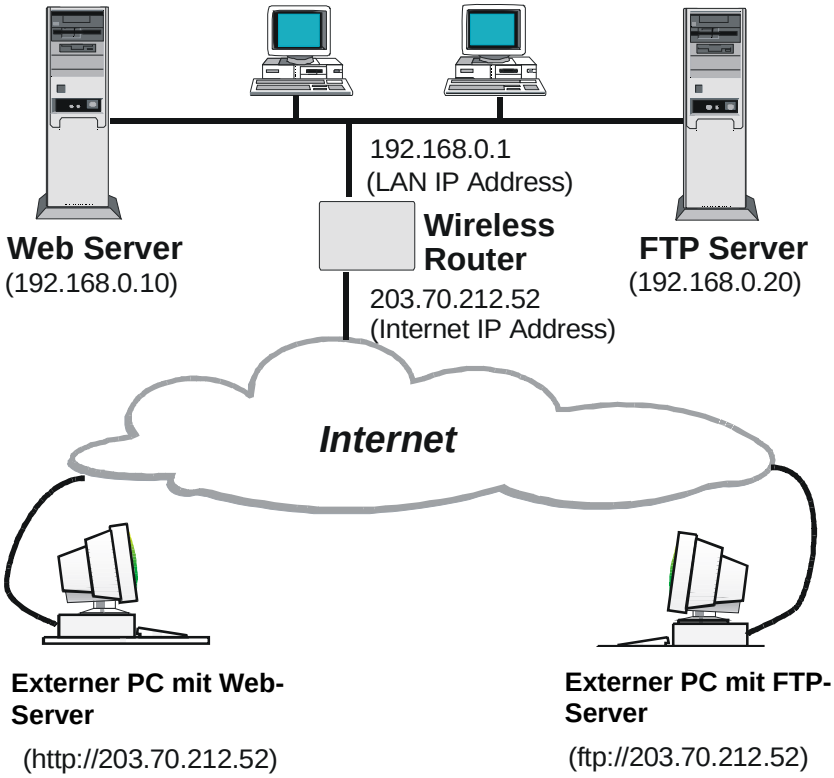


Abb. 40 Virtuelle Server

9.7.1. IP-Adresse ist für Internetnutzer einsehbar

Beachten Sie, dass sich in dieser Darstellung beide Internetnutzer mit derselben IP-Adresse verbinden, jedoch unterschiedliche Protokolle verwenden.

Für Internetnutzer haben alle virtuellen Server in Ihrem LAN dieselbe IP-Adresse. Diese IP-Adresse wird von Ihrem ISP zugeordnet.

Diese Adresse sollte statisch sein, nicht dynamisch, um Internetnutzern die Verbindung zu Ihren Servern zu erleichtern.

Sie können jedoch die *DDNS (Dynamic DNS)*-Funktion verwenden, um Internetnutzern zu gestatten, über eine URL (und nicht über eine IP-Adresse) eine Verbindung zu Ihren virtuellen Servern herzustellen.

9.7.2. Bildschirmanzeige Virtuelle Server

- Die Funktion „Virtual Server“ ermöglicht es Internetnutzern, auf die Internetserver auf Ihrem LAN zuzugreifen.
- Auf Ihren PCs muss die geeignete Serversoftware installiert sein.
- Für Internetnutzer haben ALLE Ihre Server dieselbe IP-Adresse. Diese IP-Adresse wird von Ihrem ISP zugeordnet.
- Sie können die DDNS-Funktion nutzen, um Internetnutzern die Verbindung zu Ihren Servern zu erleichtern. Dadurch können sich Internetnutzer über eine URL anstelle einer IP-Adresse eine Verbindung zu Ihren Servern herstellen. Diese Technologie funktioniert auch dann, wenn Ihr ISP Ihnen eine dynamische IP-Adresse zuweist. (Da die Zuweisung bei jedem Verbindungsaufbau erfolgt, kann sich die IP-Adressebei jedem Verbindungsaufbau ändern.)

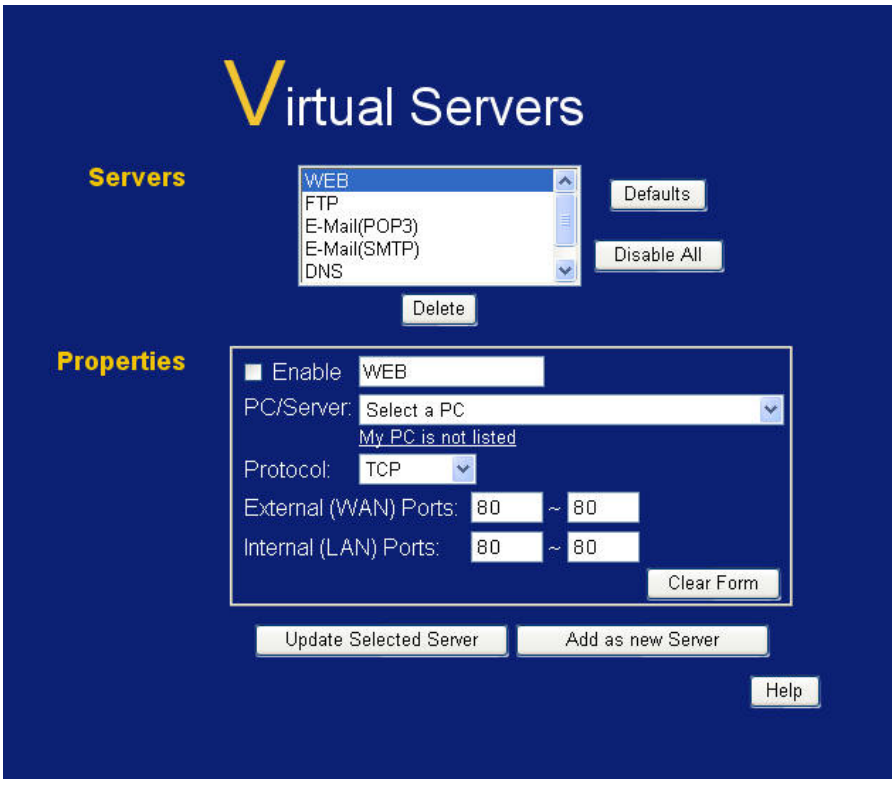


Abb. 41 Bildschirmanzeige Virtuelle Server

Daten - Bildschirmanzeige Virtuelle Server

Servers	
Servers	Diese Liste enthält eine Reihe von gängigen Server-Typen. Wenn der gewünschte Server-Typ nicht in der Liste enthalten ist, erreichen Sie über die Definition einer Firewall-Regel den gleichen Effekt wie über die “Virtual Server”-Funktion.
Properties	
Enable	Über dieses Kontrollkästchen können Sie je nach Bedarf die Serverunterstützung aktivieren oder deaktivieren. Wenn diese Funktion aktiviert ist, müssen Sie einen PC bestimmen, an den die Daten gesendet werden sollen.
PC/Server	Wählen Sie den PC für diesen Server aus. Die korrekte Serversoftware muss auf dem PC laufen.
Protocol	Wählen Sie das vom Server benutzte Protokoll (TCP, UDP, TCP/ UDP).
External Ports	Geben Sie den Zahlenbereich für externe Ports ein.
Internal Ports	Geben Sie den Zahlenbereich für interne Ports ein.
Schaltflächen	
Defaults	Dadurch werden alle von Ihnen definierte Server gelöscht und vordefinierte Server so eingestellt, dass sie ihre Vorgabe-Portnummern benutzen.
Disable All	Deaktiviert alle virtuellen Server.
Update Selected Server	Aktualisieren des gegenwärtigen Eintrags für virtuelle Server unter Nutzung der Daten unter den Eigenschaften auf dem Bildschirm.
Add as new Server	Machen Sie einen neuen Eintrag in der Liste der virtuellen Server mit den Daten aus den Eigenschaften auf dem Bildschirm. Der in der Liste ausgewählte Eintrag wird ignoriert und nicht geändert.
Delete	Löscht den ausgewählten Eintrag in der Liste der virtuellen Server. Beachten Sie, dass die vordefinierten Server nicht gelöscht werden können. Nur Server, die Sie selbst definiert haben, können gelöscht werden.
Clear Form	Löscht alle Daten aus den Eigenschaften. Ein neuer Eintrag kann vorgenommen werden.

Für jeden Eintrag muss die korrekte Serversoftware auf dem PC laufen.

9.7.3. Definition Ihrer eigenen virtuellen Server

Wenn der Servertyp, den Sie benutzen möchten, nicht auf der Bildschirmanzeige *Virtuelle Server* zu sehen ist, können Sie Ihren eigenen Server definieren und verwalten:

Create a new Server:

1. Klicken Sie auf „Clear Form“.
2. Geben Sie, wie oben beschrieben, die erforderlichen Daten ein.
3. Klicken Sie auf „Add“.
4. Der neue Server erscheint nun in der Liste.

Modify (Edit) a Server:

1. Wählen Sie den gewünschten Server aus der Liste.
2. Führen Sie gewünschte Änderungen durch (ändern Sie beispielsweise die Einstellungen zum Aktivieren / Deaktivieren).
3. Klicken Sie auf „Update Selected Server", um die Änderungen für den ausgewählten Server zu speichern.

Delete a Server:

1. Wählen Sie einen Servereintrag aus der Liste.
2. Klicken Sie auf „Delete“.

Hinweis: Sie können nur Server löschen, die Sie selbst definiert haben. Vordefinierte Server können nicht gelöscht werden.

Vom Internet haben ALLE virtuellen Server IP-Adressen, die von ihrem ISP zugeordnet wurden.

9.7.4. Verbindungsaufbau zu den virtuellen Servern

Einmal konfiguriert, kann jeder im Internet eine Verbindung zu Ihren virtuellen Servern herstellen. Dabei muss die Internet-IP-Adresse (die IP-Adresse, die von Ihrem ISP zugeordnet wurde) verwendet werden, z. B.

http://203.70.212.52

ftp://203.70.212.52

Es ist komfortabler, statt einer dynamischen eine statische IP-Adresse Ihres ISPs zu verwenden. Sie können jedoch die Funktion *Dynamic DNS* verwenden, um Internetnutzern zu gestatten, über eine URL (und nicht über eine IP-Adresse) eine Verbindung zu Ihren virtuellen Servern herzustellen.

9.8. Optionen

In diesem Bildschirm können erfahrene Anwender diverse Einstellungen eingeben oder ändern. Für den Normalbetrieb ist es nicht notwendig, diesen Bildschirm zu verwenden oder Einstellungen zu ändern. Ein Beispiel für die Bildschirmanzeige ***Optionen*** finden Sie weiter unten.

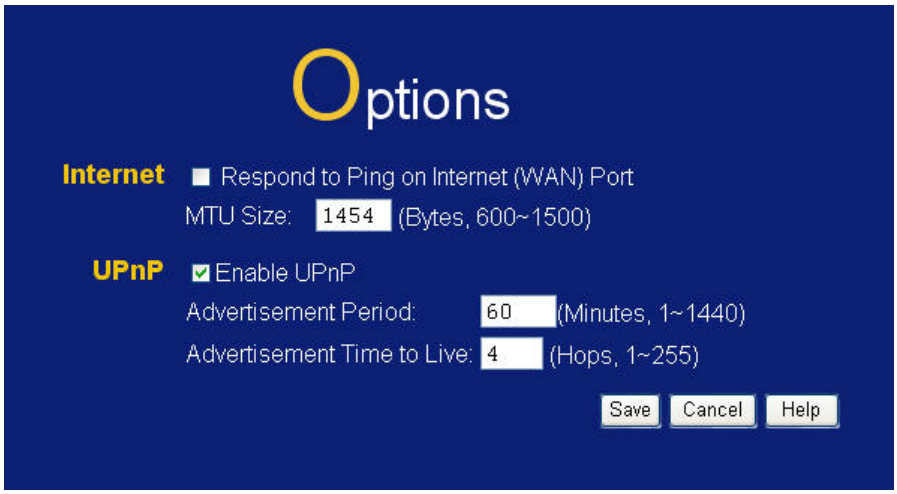


Abb. 42 Bildschirmanzeige Optionen

Daten - Bildschirmanzeige Optionen

Internet	
Respond to Ping	• Wenn dieses Kontrollkästchen aktiviert ist, antwortet der WLAN-Router auf eingehende Ping-Pakete (ICMP) aus dem Internet. • Wenn dieses Kontrollkästchen nicht aktiviert ist, werden Ping-Pakete (ICMP) aus dem Internet ignoriert. Durch Deaktivieren dieser Option erhöhen Sie geringfügig die Sicherheit Ihres Netzwerks.
MTU Size	Geben Sie hier einen Wert zwischen 1 und 1500 ein. **Hinweis:** Die MTU-Größe (Maximum Transmission Unit) sollten Sie nur auf Anraten eines Sachkundigen ändern.

UPnP	
UPnP	• UPnP (Universal Plug and Play) ermöglicht automatisches Lokalisieren und Konfigurieren von Geräten, die mit Ihrem LAN verbunden sind. UPnP wird von Windows ME, XP, oder späteren Versionen unterstützt. • Wenn ein Gerät aktiviert ist, ist es über UPnP sichtbar. • Wenn ein Gerät deaktiviert ist, ist es über UpnP nicht sichtbar.
Advertisement Period	Geben Sie hier den gewünschten Wert in Minuten ein. Der gültige Wertebereich liegt zwischen 1 und 1440.
Advertisement Time to Live	Geben Sie hier den gewünschten Wert in Hops ein. Der gültige Wertebereich liegt zwischen 1 und 255.

9.9. Port Trigger

Dieser Bildschirm kann für den Port Trigger verwendet werden.

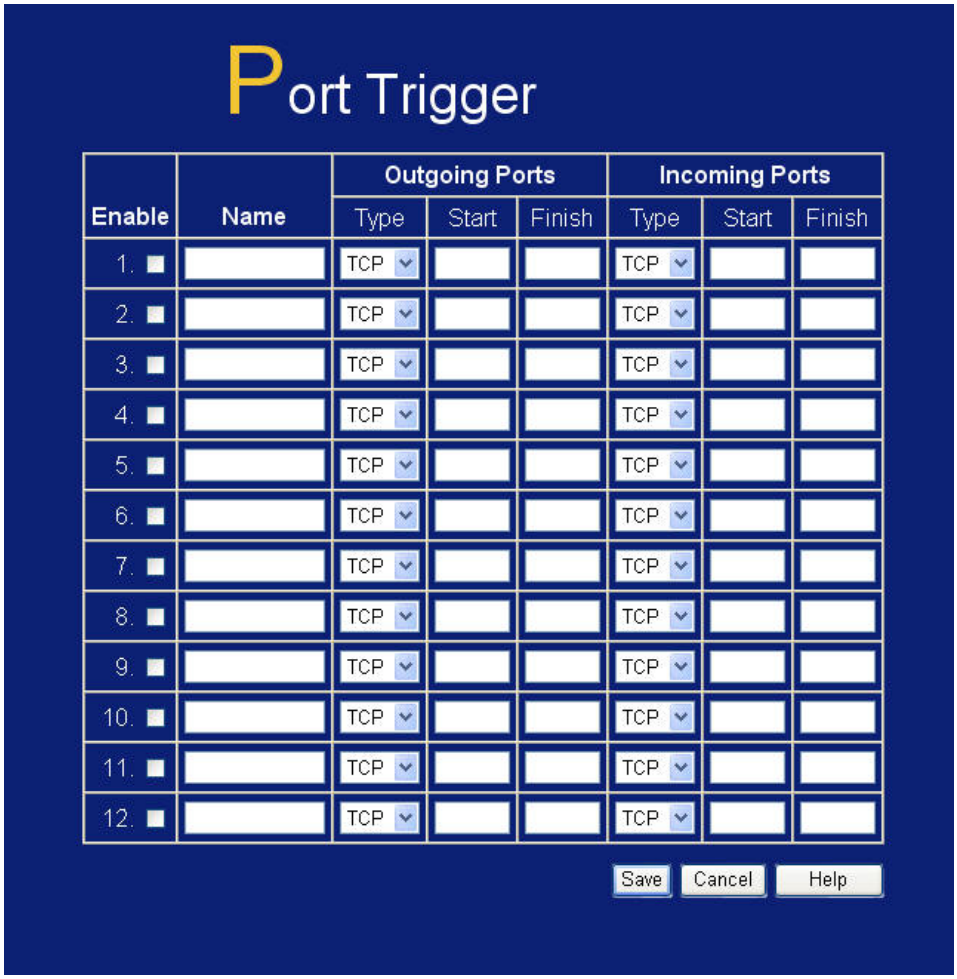


Abb. 43 Bildschirmanzeige Port Trigger

9.10. Zeitpläne

Dieser Zeitplan kann für die Firewall-Regeln und für den URL-Filter verwendet werden.

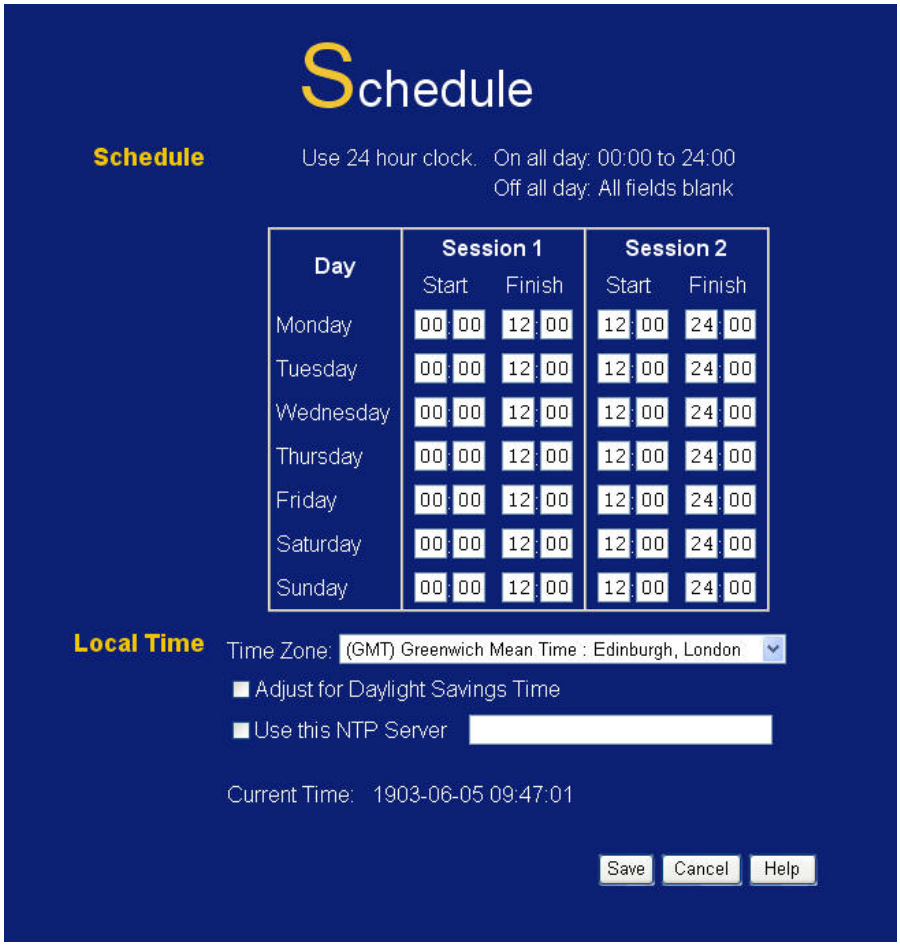


Abb. 44 Bildschirmanzeige Zeitpläne

Daten - Bildschirmanzeige Zeitpläne

Zeitpläne	
Day	Sie können für jeden Wochentag einen eigenen Zeitplan erstellen.
Session 1 **Session 2**	Es können zwei gesonderte Sitzungen oder Zeitbereiche definiert werden. Sitzung 2 muss nicht definiert werden, wenn sie nicht erforderlich ist.
Start Time	Geben Sie hier die Anfangszeit ein (24-Stunden-System).
Finish Time	Geben Sie hier die Endzeit ein (24-Stunden-System).

Local Time	
Time Zone	Damit Ihre Ortszeit korrekt angezeigt wird, müssen Sie die richtige Zeitzone aus dieser Liste auswählen.
Adjust for Daylight Savings Time	Dieses Kontrollkästchen muss zu Beginn der Sommerzeit manuell aktiviert und nach Ende der Sommerzeit wieder deaktiviert werden.
Use this NTP Server	Sollten Sie einen bestimmten NTP-Server als Primärserver bevorzugen, aktivieren Sie dieses Kontrollkästchen und tragen Sie die IP-Adresse des Servers in die nebenstehenden Felder ein. Wenn das Kontrollkästchen nicht aktiviert ist, wird der Standard-NTP-Server verwendet.
Current Time	Hier wird die aktuelle Zeit des WLAN-Breitbandrouters angezeigt, wenn die Seite geladen wird.

10. Erweiterte Verwaltung

Dieses Kapitel beschreibt die im Menüabschnitt „Verwaltung" zu Verfügung stehenden Einstellungen.

10.1. Übersicht

Es ist für gewöhnlich nicht erforderlich, auf diese Bildschirme zuzugreifen oder an den Einstellungen etwas zu ändern. Diese Bildschirme und Einstellungen dienen ausschließlich dazu, außergewöhnliche Situationen zu bewältigen und erfahrenen Anwendern zusätzliche Optionen zur Verfügung zu stellen.

Folgende Einstellungen und Funktionen sind verfügbar:

PC-Datenbank	Diese Liste der PCs wird angezeigt, wenn Sie den „DMZ-PC" oder einen virtuellen Server auswählen. Diese Datenbank wird automatisch verwaltet, Sie können jedoch Einträge für PCs, die eine statische IP-Adresse nutzen, hinzufügen und löschen.
Diagnose	Durchführen von Ping oder DNS-Lookup.
Konfigurationsdatei	Sichern oder Wiederherstellen der Konfigurationsdatei für den WLAN-Breitbandrouter. Diese Datei enthält alle Konfigurationsdaten.
Logs	Ansicht oder Löschen aller Log-Dateien, Einstellung der E-Mail-Funktion für Log-Dateien und Warnmeldungen.
Externe Verwaltung	Ändern von Einstellungen über das Internet.
Firmware-Upgrade	Upgrade der Firmware (Software) auf Ihrem WLAN-Breitbandrouter

10.2. PC-Datenbank

In dieser Bildschirmanzeige wird das Gerät angezeigt, das eine Verbindung mit dem Router herstellt.

- IP-Adressen müssen nicht mehr angegeben werden.
- Außerdem müssen in Ihrem LAN auch keine festen IP-Adressen verwendet werden.

10.2.1. Bildschirmanzeige PC-Datenbank

In der nachstehenden Abbildung sehen Sie ein Beispiel für eine ***PC-Datenbank***.

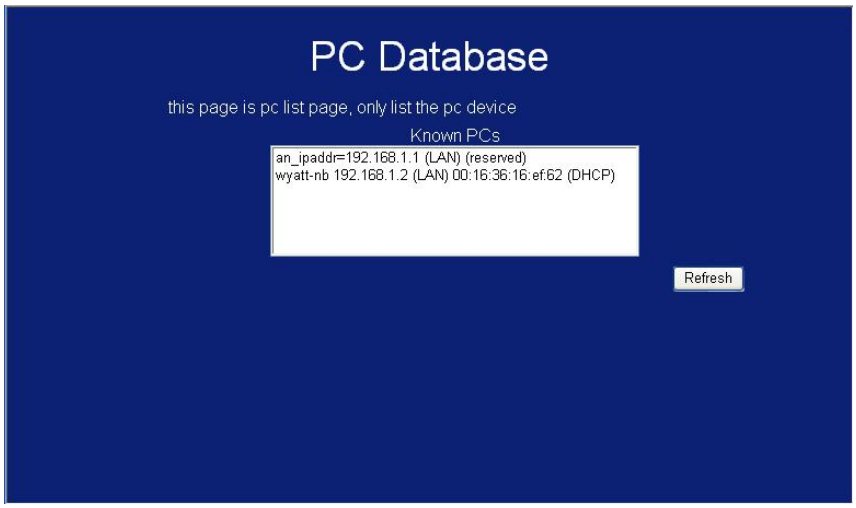

PC Database
this page is pc list page, only list the pc device
Known PCs
an_ipaddr=192.168.1.1 (LAN) (reserved)
wyatt-nb 192.168.1.2 (LAN) 00:16:36:16:ef:62 (DHCP)
Refresh

Abb. 45 Bildschirmanzeige PC-Datenbank

- PCs, bei denen es sich um DHCP-Clients handelt, werden der Datenbank automatisch hinzugefügt und nach Notwendigkeit aktualisiert.
- Vorgabegemäß fungieren Nicht-Server-Versionen von Windows als DHCP-Clients. Diese Einstellung wird "IP-Adresse automatisch beziehen" genannt.
- Der WLAN-Breitbandrouter verwendet zur Identifikation jedes PCs die Hardwareadresse und nicht den Namen oder die IP-Adresse. Die Hardwareadresse kann nur geändert werden, wenn Sie die Netzwerkkarte oder den Adapter des PCs austauschen.Daten - Bildschirmanzeige PC-Datenbank

Known PCs	Hier sind alle aktuellen Einträge aufgelistet. Bei den angezeigten Daten handelt es sich um den *Namenstyp (IP-Adresse)*. Der Typ zeigt an, ob der PC am LAN angeschlossen ist.
Schaltflächen	
Refresh	Über diese Schaltfläche aktualisieren Sie die Daten auf dem Bildschirm.

10.3. Diagnose

Über diese Bildschirmanzeige können Sie einen Ping- oder DNS-Lookup-Befehl ausführen. Diese Optionen dienen der Fehlersuche bei Netzwerkproblemen.

Die nachstehende Abbildung zeigt die Bildschirmanzeige ***Netzwerkdiagnose***.

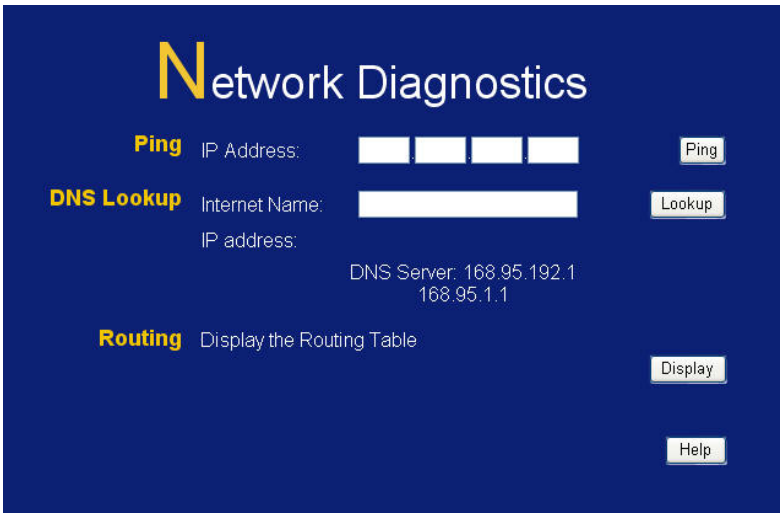


Abb. 46 Bildschirmanzeige Netzwerkdiagnose

Daten - Bildschirmanzeige Netzwerkdiagnose

Ping	
Ping this IP Address	Geben Sie hier die IP-Adresse ein, die gepingt werden soll. Diese IP-Adresse kann sich in Ihrem LAN oder im Internet befinden. Wenn sich die Adresse im Internet befindet und gerade keine Internetverbindung zu dem entsprechenden Gerät besteht, kann es zu einer „Timeout"-Fehlermeldung kommen. Warten Sie in diesem Fall einige Sekunden und versuchen Sie es dann erneut.
Ping	Geben Sie die IP-Adresse ein und klicken Sie dann auf diese Schaltfläche, um den Ping-Vorgang zu starten. Die Ergebnisse werden im Feld *Ping Results* angezeigt.
DNS Lookup	
Internet name	Geben Sie den Domainnamen oder die URL ein, für die eine DNS-Suche (Domain Name Server) durchgeführt werden soll. Wenn sich die Adresse im Internet befindet und gerade keine Internetverbindung zu dem entsprechenden Gerät besteht, kann es zu einer „Timeout"-Fehlermeldung kommen. Warten Sie in diesem Fall einige Sekunden und versuchen Sie es dann erneut.
Lookup	Durch Klicken auf diese Schaltfläche nach Eingabe des Domainnamens bzw. der URL wird die Suche gestartet.
Routing	
Display	Durch Klicken auf diese Schaltfläche wird die Internet-Routing-Tabelle angezeigt. Die angezeigten Informationen sind für Personen mit entsprechenden Kenntnissen von Nutzen.

10.4. Konfigurationsdatei

Diese Funktion ermöglicht es, die aktuellen Einstellungen des WLAN-Breitbandrouters herunterzuladen und diese als Datei auf Ihrem PC zu speichern.

Eine auf diese Weise gespeicherte Konfiguration kann durch das Hochladen der Datei auf den WLAN-Breitbandouter wiederhergestellt werden.

Darüber hinaus können Sie auf diesem Bildschirm die werkseitige Standardkonfiguration des WLAN-Breitbandrouters wiederherstellen. Sämtliche bestehenden Einstellungen werden dabei gelöscht.

Die nachstehende Abbildung zeigt eine ***Konfigurationsdatei***.

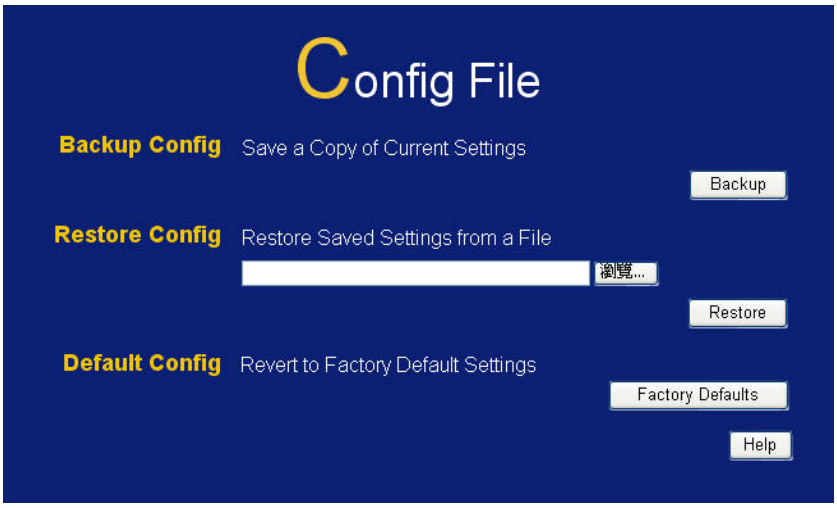


Abb. 47 Bildschirmanzeige Konfigurationsdatei

Daten - Bildschirmanzeige Konfigurationsdatei

Backup Config	Hier können Sie die aktuelle Konfiguration herunterladen und als Datei auf Ihrem PC speichern. Klicken Sie auf *Backup*, um den Download zu starten.
Restore Config	Hier können Sie eine gespeicherte Konfiguration durch Hochladen der Datei auf den WLAN-Breitbandrouter wiederherstellen. Klicken Sie auf *Browse*, um die Konfigurationsdatei auszuwählen und dann auf *Restore*, um den Upload zu starten. **WARNUNG!** Durch das Hochladen einer Konfigurationsdatei werden ALLE bestehenden Einstellungen überschrieben und gehen damit verloren.
Default Config	Klicken Sie auf *Factory Defaults*, um die werkseitigen Standardeinstellungen des WLAN-Breitbandrouters wiederherzustellen. **WARNUNG!** Hierdurch werden ALLE bestehenden Einstellungen gelöscht.

10.5. Logs

Log-Dateien protokollieren verschiedene Aktivitäten auf dem WLAN-Breitbandrouter. Diese Daten sind sehr nützlich zur Fehlerbehebung. Wenn jedoch alle Logs aktiv sind, entsteht eine große Datenmenge, die die Leistung negativ beeinflussen kann.

Logs
Logs
Current time: 1903-06-05 09:49:42
[Dhcp] Fri 1903-06-05 08:11:00 192.168.1.2 0
[Login] Fri 1903-06-05 08:11:26 syslog: [Logi
[Logout] Fri 1903-06-05 08:11:49 syslog: [Log
[Logout] Fri 1903-06-05 08:11:49 syslog: [Log
[Login] Fri 1903-06-05 08:20:09 syslog: [Logi
[Logout] Fri 1903-06-05 08:20:18 syslog: [Log
[Bootup] Fri 1903-06-05 08:20:28 - Router sta
[Dhcp] Fri 1903-06-05 08:20:44 192.168.1.2 0
[Wan] Fri 1903-06-05 08:22:01 WAN DHCP Client
[Login] Fri 1903-06-05 08:25:22 syslog: [Logi
[Logout] Fri 1903-06-05 08:47:56 syslog: [Log
[Login] Fri 1903-06-05 08:47:59 syslog: [Logi
Refresh
Clear Log
Send Log
Include in Log
Attempted access to blocked sites
Connections to the Web-based interface of this Router
Router operation (start up, get time etc)
Known DoS attacks and Port Scans
Syslog
Disable
Broadcast on LAN
Send to this Syslog Server:
Save
Cancel
Help

Abb. 48 Bildschirmanzeige Logs

Daten - Bildschirmanzeige Logs

Logs	
Current Time	Hier wird die aktuelle Zeiteinstellung des WLAN-Breitbandrouters angezeigt.
Log Data	In diesem Fenster werden aktuelle Log-Daten angezeigt.
Refresh	Mit dieser Schaltfläche können Sie Log-Daten aktualisieren.

10.6. Externe Verwaltung

Wenn aktiviert, ermöglicht diese Funktion die Verwaltung des WLAN-Breitbandrouters über das Internet.

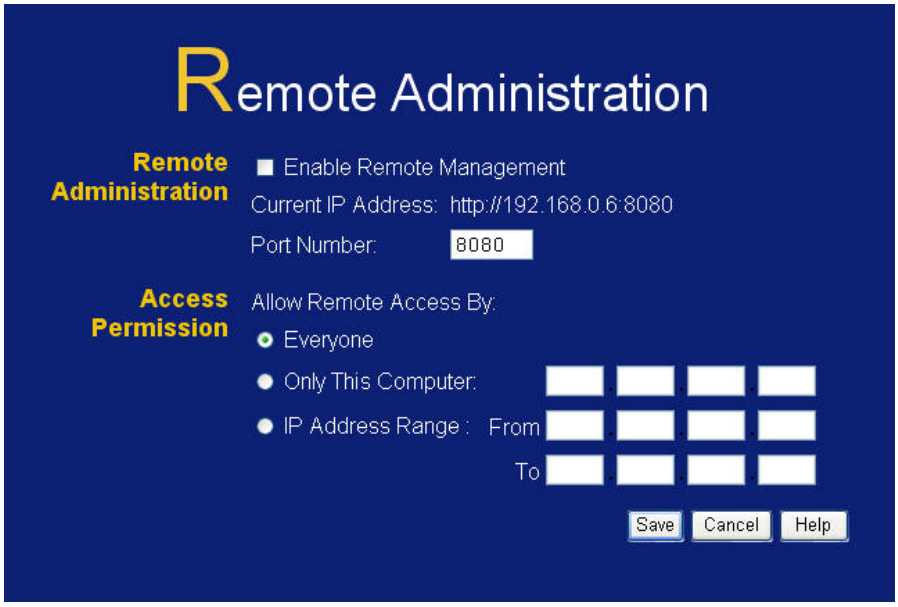


Abb. 49 Bildschirmanzeige Externe Verwaltung

Daten - Bildschirmanzeige Externe Verwaltung

Externe Verwaltung	
Enable Remote Management	Aktivieren Sie dieses Kontrollkästchen, um die Verwaltung über das Internet zu ermöglichen. (Nähere Informationen über das Herstellen der Verbindung, siehe unten.) Wenn deaktiviert, ist keine externe Verwaltung möglich.
Current IP Address	Hierbei handelt es sich um die aktuelle IP-Adresse, die Sie beim Zugriff auf das Gerät über das Internet nutzen. Weiter unten wird exemplarisch erläutert, wie die Verbindung hergestellt wird.
Port Number	Geben Sie hier eine Portnummer zwischen 1 und 65535 ein. Der Standard-Port für HTTP (Internet)-Verbindungen ist Port 80, aber eine Verwendung von Port 80 an dieser Stelle verhindert die Verwendung eines „virtuellen Servers“ für das Internet in Ihrem LAN. Aus diesem Grund wird empfohlen, eine andere Portnummer einzutragen. Der Vorgabewert ist 8080. Diese Portnummer muss beim Verbindungsaufbau in Ihrem Browser festgelegt sein. Näheres hierzu erfahren Sie im folgenden Abschnitt.

Herstellung einer Verbindung von einem externen PC über das Internet

1. Stellen Sie sicher, dass eine Internetverbindung besteht und starten Sie ihren Web-Browser.
2. Geben Sie in der Adressleiste „HTTP://" ein, gefolgt von der Internet-IP-Adresse des WLAN-Breitbandrouters. Wenn die Portnummer nicht 80 ist, wird die Portnummer ebenfalls benötigt. (Geben Sie nach der IP-Adresse „:“ ein, gefolgt von der Portnummer)
   z. B.

   HTTP://123.123.123.123:8080y

In diesem Beispiel wird angenommen, dass die WAN-IP-Adresse 123.123.123.123 lautet und die Portnummer 8080 ist.

3. Sie werden anschließend aufgefordert, den Login-Namen und das Passwort für das Gerät einzugeben.

10.7. Firmware-Upgrade

Die Firmware (Software) des WLAN-Breitbandrouters kann über den Web-Browser aktualisiert werden. Sie müssen zunächst die Upgrade-Datei herunterladen und dann *Upgrade Firmware* im *Verwaltungsmenü* auswählen. Folgender Bildschirm öffnet sich.

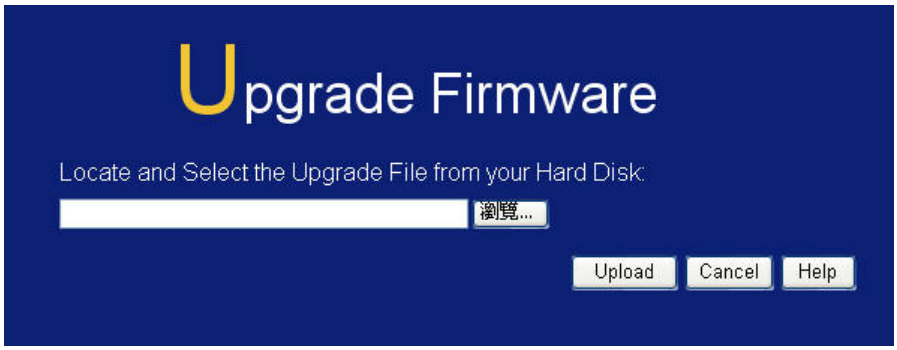


Abb. 50 Bildschirmanzeige Firmware-Upgrade

Gehen Sie folgendermaßen vor, um ein Firmware-Upgrade durchzuführen:

1. Klicken Sie auf *Browse* und navigieren Sie zu der Upgrade-Datei.
2. Wählen Sie eine Upgrade-Datei aus. Der Dateiname erscheint im Auswahlfeld *Upgrade File*.
3. Klicken Sie auf *Upload*, um das Firmware-Upgrade zu starten.

Während das Upgrade durchgeführt wird, kann der WLAN-Breitbandrouter nicht genutzt werden. Nach dem Upgrade ist ein Neustart erforderlich. Bestehende Verbindungen zum oder über den WLAN-Breitbandrouter werden abgebrochen.

11. Fehlersuche und -behebung

Dieser Anhang beschreibt die häufigsten Probleme und deren Lösungen.

11.1. Übersicht

Dieses Kapitel behandelt Problemfälle, die häufig bei der Nutzung des WLAN-Breitbandrouters auftreten und gibt Lösungsvorschläge. Wenn Sie die angegebenen Lösungsansätze befolgen und der WLAN-Breitbandrouter noch immer nicht richtig funktioniert, wenden Sie sich bitte an Ihren Händler.

11.2. Allgemeine Probleme

Problem 1:	**Es kann keine Verbindung mit dem WLAN-Breitbandrouter hergestellt werden, um ihn zu konfigurieren.**
Lösung 1:	Prüfen Sie folgende Punkte: • Ist der WLAN-Breitbandrouter korrekt installiert, die LAN-Verbindungen OK, und das Gerät eingeschaltet? • Stellen Sie sicher, dass sich Ihr PC und der WLAN-Breitbandrouter im selben Netzwerksegment befinden. (Wenn Sie keinen Router verwenden, sollte dies der Fall sein.) • Falls Ihr PC auf „IP-Adresse automatisch beziehen" (DHCP-Client) eingestellt ist, starten Sie ihn erneut. • Falls Ihr PC eine feste (statische) IP-Adresse verwendet, stellen Sie sicher, dass die IP-Adresse im Bereich zwischen 192.168.0.2 und 192.168.0.254 liegt, um mit der Vorgabe-IP-Adresse des WLAN-Breitbandrouters (192.168.0.1) kompatibel zu sein. Die Netzwerkmaske sollte außerdem auf 255.255.255.0 eingestellt sein, um mit der des WLAN-Breitbandrouters übereinzustimmen. In Windows können Sie diese Einstellungen unter *Netzwerkeinstellungen* und *Eigenschaften* des Internetprotokolls (TCP/IP) überprüfen.

11.3. Internetzugang

Problem 1:	**Bei Eingabe einer URL oder IP-Adresse erscheint ein Timeout-Fehler.**
Lösung 1:	Dieser Fehler kann eine Reihe von Ursachen haben. Gehen Sie die folgenden Schritte zur Fehlerbehebung durch. • Überprüfen Sie, ob die anderen PCs funktionieren. Ist dies der Fall, sollten Sie sicherstellen, dass die IP-Einstellungen Ihres PCs korrekt sind. Falls Sie eine feste (statische) IP-Adresse benutzen, prüfen Sie Netzwerkmaske, Standard-Gateway, DNS und IP-Adresse. • Wenn die PCs korrekt konfiguriert sind, aber noch immer nicht funktionieren, überprüfen Sie den WLAN-Breitbandrouter. Stellen Sie sicher, dass eine Verbindung besteht und der Router eingeschaltet ist. Stellen Sie eine Verbindung zum WLAN-Breitbandrouter her und überprüfen Sie dessen Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie das LAN und die Stromverbindungen). • Überprüfen Sie auf dem Status-Bildschirm, ob der WLAN-Breitbandrouter korrekt funktioniert.
Problem 2:	**Einige Anwendungen funktionieren nicht einwandfrei, wenn der WLAN-Breitbandrouter benutzt wird.**
Lösung 2:	Der WLAN-Breitbandrouter verarbeitet die über Ihn geleiteten Daten, ist also nicht transparent. Für eingehende Verbindungen müssen Sie „Virtual Server" oder die Firewall-Regeln verwenden, um zu bestimmen, welcher PC den eingehenden Verkehr empfangen soll. Sie können auch die *DMZ*-Funktion nutzen. Diese funktioniert praktisch mit allen Anwendungen. Allerdings: • stellt dies ein Sicherheitsrisiko dar, da die Firewall deaktiviert wird, • kann nur ein PC diese Funktion zu einem Zeitpunkt verwenden.

11.4. WLAN-Zugang

Problem 1:	**Der PC kann den Wireless Access Point nicht finden.**

Lösung 1: Prüfen Sie folgende Punkte:

- Läuft der PC im *Infrastruktur-Modus*? (Access Points sind stets im *Infrastruktur-Modus*)
- Sind die SSID Ihres PCs und die des Wireless Access Points identisch?
  Achten Sie auf Groß- und Kleinschreibung. Das Wort „Workgroup" entspricht folglich NICHT dem Wort „workgroup".
- Die WEP-Einstellungen für PC und WLAN-Breitbandrouter müssen identisch sein. WEP ist beim WLAN-Breitbandrouter standardmäßig nicht aktiviert und sollte folglich auch bei Ihrer WLAN-Station nicht aktiviert sein.
- Sollte WEP jedoch beim WLAN-Breitbandrouter aktiviert sein, muss auch bei Ihrem PC diese Funktion aktiviert, sowie der gleiche Schlüssel konfiguriert sein.
- Wenn auf der Bildschirmanzeige des WLAN-Breitbandrouters - *Wireless* - *Allow* eingestellt ist, müssen alle WLAN-Stationen als „Trusted" gekennzeichnet sein. Ansonsten haben Sie keinen Zugang.
- Um zu überprüfen, ob Hochfrequenzstrahlung Probleme verursacht, prüfen Sie, ob eine Verbindung nahe am WLAN-Breitbandrouter möglich ist.
  Beachten Sie, dass die Verbindungsreichweite bei ungünstigen Bedingungen nur ca. 30 m betragen kann.

Problem 2:	Die Geschwindigkeit der WLAN-Verbindung ist sehr langsam.
Lösung 2:	Die Geschwindigkeit der Verbindung hängt von der Entfernung des Routers und den Umgebungsbedingungen ab. Probieren Sie Folgendes, um eine maximale Verbindungsgeschwindigkeit zu erreichen:

- Standort des WLAN-Breitbandrouters
  Verändern Sie den Standort und die Ausrichtung des WLAN-Breitbandrouters.
- WLAN-Kanal
  Wenn Störungen auftreten, kann es hilfreich sein, den Kanal zu wechseln.
- Hochfrequenzstrahlung
  Die Störung kann von anderen Geräten ausgehen. Schalten Sie diese Geräte probeweise aus, um herauszufinden, ob Sie wirklich die Ursache für die Störung sind. Geräte mit einem hohen Geräuschpegel sollten abgeschirmt oder woanders aufgestellt werden.
- Hochfrequenzabschirmung
  Je nach Umgebung ist es möglich, dass die Übertragung zwischen WLAN-Stationen blockiert wird. In diesem Fall sind hohe Verbindungsgeschwindigkeiten nur in unmittelbarer Nähe des WLAN-Breitbandrouters möglich.

12. Wireless LANs

Dieser Anhang enthält Hintergrundinformationen über die Wireless LANs (WLANs) und deren Nutzung.

12.1. Modi

Infrastruktur-Modus

Im Infrastruktur-Modus werden ein oder mehrere Access Points verwendet, um WLAN-Stationen (z. B. Notebooks mit WLAN-Karte) zu einem Ethernet-LAN zu verbinden. Diese WLAN-Stationen können dann alle LAN-Ressourcen nutzen.

Access Points funktionieren ausschließlich im Infrastruktur-Modus und können nur mit WLAN-Stationen kommunizieren, die sich ebenfalls im Infrastruktur-Modus befinden.

12.2. BSS/ESS

BSS

Eine Gruppe bestehend aus WLAN-Stationen und einem einzelnen Access Point, die den gleichen Netzwerknamen verwenden, bildet ein so genanntes Basic Service Set (BSS).

Voraussetzung ist hierbei die Nutzung desselben Netzwerknamens. Geräte, die unterschiedliche Netzwerknamen nutzen, können nicht miteinander kommunizieren.

ESS

Eine Gruppe bestehend aus WLAN-Stationen und mehreren Access Points, die die gleiche ESSID nutzt, bildet ein so genanntes Extended Service Set (ESS).

Innerhalb eines ESS können unterschiedliche Access Points unterschiedliche Kanäle nutzen. Insbesondere für benachbarte Access Points ist dies sogar ratsam, um Interferenzen zu minimieren.

Wenn innerhalb der Reichweite eines ESS der Standort von WLAN-Stationen geändert wird, dann wechseln diese automatisch zu dem Access Point, der die geringste Interferenz bzw. beste Verbindung ermöglicht. Dieses Verhalten wird als **Roaming** bezeichnet (Access Points haben und benötigen kein Roaming).

12.3. Kanäle

Der WLAN-Kanal bestimmt die Übertragungsfrequenz.

- Jeder Access Point nutzt einen festen Kanal. Sie können diese Kanäle einstellen. Dadurch haben Sie die Möglichkeit, Kanäle mit der geringsten Interferenz und besten Übertragung auszuwählen. In den USA und in Kanada stehen elf Kanäle zur Verfügung. Wenn Sie mehrere Access Points verwenden, ist es zwecks Reduzierung von Interferenzen ratsam, für benachbarte Access Points unterschiedliche Kanäle einzustellen.
- Im Infrastruktur-Modus scannen die WLAN-Stationen normalerweise sämtliche Kanäle, um einen Access Point zu finden. Wenn mehrere Access Points zur Auswahl stehen, wird derjenige mit dem stärksten Signal genutzt. (Dies ist nur innerhalb eines ESS möglich.)
- Im Ad-Hoc-Modus (kein Access Point), sollten alle WLAN-Stationen so eingestellt sein, dass sie den gleichen Kanal nutzen. Auch dann werden jedoch die meisten WLAN-Stationen nach wie vor alle Kanäle scannen, um herauszufinden, ob eine Verbindung zu einer bestehenden Ad-Hoc-Gruppe aufgebaut werden kann.

12.4. WEP

WEP (Wired Equivalent Privacy) ist ein Standard zur Verschlüsselung von Daten.

Daten sollten vor der Übertragung verschlüsselt werden, da es grundsätzlich nicht möglich ist, den Datenverkehr zwischen WLAN-Stationen vor „Schnüfflern“ abzuschirmen. Wenn die Daten jedoch verschlüsselt wurden, sind diese für Dritte unbrauchbar, es sei denn, der Empfänger kann sie entschlüsseln.

Wenn WEP verwendet wird, müssen folgende Einstellungen bei den WLAN-Stationen und dem Access Point übereinstimmen.

WEP	Off, 64 Bit, 128 Bit
Key	Bei 64-Bit-Verschlüsselung muss der Schlüsselwert übereinstimmen. Bei 128-Bit-Verschlüsselung muss der Schlüsselwert übereinstimmen.
WEP-Authentifizierung	„Open System“ oder „Shared Key“

12.5. WPA-PSK

Auch bei WPA-PSK handelt es sich um einen Standard, der zur Datenverschlüsselung vor dem Senden verwendet wird. Dieser Standard ist aktueller als WEP (Wired Equivalent Privacy) und bietet daher mehr Sicherheit. Die Daten werden mit einem Schlüssel verschlüsselt, der automatisch generiert und oft verändert wird.

Wenn alle WLAN-Stationen WPA-PSK unterstützen, sollten sie WPA-PSK anstelle von WEP verwenden.

Wenn WPA-PSK verwendet wird, müssen folgende Einstellungen bei den WLAN-Stationen und dem Access Point übereinstimmen.

WPA PSK (Pre-shared Key)	Geben Sie an jeder Station und am Access Point denselben Wert ein. Der Schlüsselwert muss eine Länge von 8 - 63 Zeichen haben. Der Schlüssel für die eigentliche Verschlüsselung wird von diesem Schlüssel abgeleitet.
Encryption	Es muss die gleiche Verschlüsselungsmethode verwendet werden. Die gebräuchlichste Methode ist TKIP. Sehr gängig ist auch AES.

12.6. Konfiguration des Wireless LAN

Um WLAN-Stationen die Verbindung zum Access Point zu ermöglichen, müssen folgende Einstellungen bei den WLAN-Stationen und dem Access Point übereinstimmen:

Modus	Bei Client-WLAN-Station muss „Infrastructure" eingestellt sein. (Der Access Point ist immer im Infrastruktur-Modus.)
SSID (ESSID)	WLAN-Stationen müssen die gleichen SSID (ESSID) verwenden, wie der Access Point, zu dem sie eine Verbindung herstellen wollen. Alternativ dazu kann der SSID-Wert auch auf „any“ gesetzt oder das Feld ganz leer bleiben, um eine Verbindung zu allen Access Points zu ermöglichen.
Wireless Security	Die WLAN-Stationen und der Access Point müssen die gleichen WLAN-Sicherheitseinstellungen verwenden (keine, WEP, WPA-PSK). **WEP** Wenn WEP verwendet wird, müssen Schlüsselgröße (64 Bit, 128 Bit), Schlüsselwert und Authentifizierungseinstellungen auf allen WLAN-Stationen und dem Access Point übereinstimmen. **WPA-PSK:** Wenn WPA-PSK verwendet wird, müssen alle WLAN-Stationen auf WPA-PSK eingestellt sein und denselben Pre-shared Key und das gleiche Verschlüsselungssystem verwenden. Bei **Ad-Hoc-Netzwerken** (kein Access Point), müssen alle WLAN-Stationen die gleichen Sicherheitseinstellungen verwenden.

13. Spezifikationen

13.1. Multifunktionaler WLAN-Breitbandrouter

Modell	LevelOne WBR-6000 *N_One* WLAN-Breitbandrouter
Abmessungen	173mm(B) * 147mm(T) * 37mm(H)
Betriebstemperatur	0° C bis 40° C
Lagertemperatur	-10° C bis 70° C
Netzwerkprotokoll:	TCP/IP
Netzwerkschnitt-stelle:	4 * 10/100BaseT (RJ45) LAN-Anschluss 1 * RJ11 für WAN-Verbindung
LEDs	6
Netzteil	12VDC 1A extern

13.2. WLAN-Schnittstelle

Normen	IEEE802.11b, IEEE802.11g WLAN, 802.11n (Entwurf)
Frequenz	2,4 bis 2,4835GHz (Industrial Scientific Medical Band)
Kanäle	Maximal 14 Kanäle, abhängig von den Regulierungsbehörden
Modulation	CCK, DQPSK, DBPSK, OFDM/CCK
Datenrate	Bis zu 300 Mbps (802.11n Draft)
Sicherheit	WEP 64Bit, 128Bit, WPA-PSK,WPA2-PSK, MAC-Adressenüberprüfung
Ausgangsleistung	13 dBm (typisch)

14. Entsorgung

Der Gesetzgeber verpflichtet uns, Sie darauf hinzuweisen, dass das Gerät hochwertige Materialien enthält, die der Wiederverwertung zugeführt werden sollen. Entsorgen Sie das Gerät daher nicht über den Hausmüll, sondern geben Sie es an einer Sammelstelle für Elektrogeräte zur Entsorgung ab.

Symbol „Elektromüll nicht über die Hausmülltonne entsorgen“

15. GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;

or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;

or,

Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

The Code for this product can be downloaded at

http://www.level1.com/support.php